MSAM, Transport Module, DMC, 40G Module, CSAM, and T-BERD 5800

Ethernet, IP, TCP/UDP, Fibre Channel, VoIP, and IP Video Testing Manual

MSAM, Transport Module, DMC, 40G Module, CSAM, and T-BERD 5800

Ethernet, IP, TCP/UDP, Fibre Channel, VoIP, and IP Video Testing Manual

JDSU
Network and Service Enablement
20250 Century Blvd
Germantown, Maryland 20874 USA
Toll Free 1-855-ASK-JDSU • Tel +1-301-353-1560 • Fax +1-240-404-1996
www.jdsu.com

Notice

Every effort was made to ensure that the information in this manual was accurate at the time of printing. However, information is subject to change without notice, and JDS Uniphase reserves the right to provide an addendum to this manual with information not available at the time that this manual was created.

Copyright

© Copyright 2015 JDS Uniphase Corporation. All rights reserved. JDSU, Network and Service Enablement, and the JDSU logo are trademarks of JDS Uniphase Corporation (“JDS Uniphase”). All other trademarks and registered trademarks are the property of their respective owners. No part of this guide may be reproduced or transmitted electronically or otherwise without written permission of the publisher.

Copyright release

Reproduction and distribution of this guide is authorized for Government purposes only.

Trademarks

JDS Uniphase, JDSU, MTS 6000A, T-BERD 6000A, MTS 8000, and T-BERD 6000A are trademarks or registered trademarks of JDS Uniphase in the United States and/or other countries.

Cisco is a registered trademark of Cisco and/or its affiliates in the U.S. and certain other countries.

NetFlow is a trademark of Cisco Systems, Inc. in the United States and certain other countries.

Wireshark is a registered trademark of the Wireshark Foundation.

All trademarks and registered trademarks are the property of their respective companies.

Terms and conditions

Specifications, terms, and conditions are subject to change without notice. The provision of hardware, services, and/or software are subject to JDSU’s standard terms and conditions, available at www.jdsu.com/terms.

FCC Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Ordering information

The catalog number for a printed getting started manual is ML-22046563. The catalog number for a printed Ethernet testing manual is ML-22046565. The catalog number for electronic manuals on USB is CEML-21138299.

WEEE and Battery Directive Compliance

JDSU has established processes in compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive, 2002/96/EC, and the Battery Directive, 2006/66/EC.

This product, and the batteries used to power the product, should not be disposed of as unsorted municipal waste and should be collected separately and disposed of according to your national regulations. In the European Union, all equipment and batteries purchased from JDSU after 2005-08-13 can be returned for disposal at the end of its useful life. JDSU will ensure that all waste equipment and batteries returned are reused, recycled, or disposed of in an environmentally friendly manner, and in compliance with all applicable national and international waste legislation.

It is the responsibility of the equipment owner to return equipment and batteries to JDSU for appropriate disposal. If the equipment or battery was imported by a reseller whose name or logo is marked on the equipment or battery, then the owner should return the equipment or battery directly to the reseller.

Instructions for returning waste equipment and batteries to JDSU can be found in the Environmental section of JDSU's web site at www.jdsu.com. If you have questions concerning disposal of your equipment or batteries, contact JDSU's WEEE Program Management team at WEEE.EMEA@jdsu.com.

Contents

About this Manual xix

Purpose and scope xx
Assumptions xx
Terminology xx
Ethernet, IP, TCP/UDP, Fibre Channel, and IP Video Testing Manual xxii
Conventions xxiii
Safety and compliance information xxiv
Technical assistance xxiv

Chapter 1 Basic Testing 1

Step 1: Selecting a test application 2
Step 2: Configuring a test 2
Step 3: Connecting the instrument to the circuit 3
Step 4: Starting the test 3
Step 5: Viewing test results 4
Setting the result group and category 4
Additional test result information 4
Running multiple tests 5

Chapter 2 Optical BERT Testing 7

About Optical BERT testing 8
BER Testing Optical Layer 1 8
Monitoring Optical Layer 1 9

Chapter 3 CPRI/OBSAI Testing 11

About CPRI/OBSAI testing . . . 12
Layer 1 CPRI or OBSAI BER Testing . . . 12
Layer 2 CPRI testing . . . 15
Inserting alarms . . . 16
Layer 2 OBSAI testing . . . 16
Inserting errors . . . 18
Monitoring CPRI or OBSAI layer 1 . . . 18

Chapter 4 Ethernet and IP Testing 21

About Ethernet and IP testing . . . 22
Features and capabilities . . . 22
Understanding the graphical user interface . . . 25
Frame settings . . . 25
Packet settings . . . 26
Ethernet and IP test applications . . . 26
MiM test applications . . . 27
MPLS-TP test applications . . . 27
PTP/1588 test applications . . . 28
Configuring applications in Dual Through mode . . . 28
Configuring 10 Gigabit Ethernet WAN tests . . . 29
Configuring Ethernet VPLS tests . . . 29
VPLS tunnels . . . 30
Virtual channels . . . 30
VPLS test applications . . . 30
Configuring MPLS over Ethernet tests . . . 30
Configuring IPv4 and IPv6 tests . . . 32
Cable Diagnostics . . . 32
Running cable diagnostics . . . 32
Viewing cable measurements . . . 33
Skew Injection . . . 33
Adjusting the frequency of transmitted optical signals . . . 34
Enabling automatic traffic transmission . . . 35
Prerequisites for traffic transmission . . . 35
Issues to consider . . . 35
Enabling the feature . . . 35
Discovering another JDSU test instrument using J-Connect . . . 36
Discoverable instruments . . . 36
Prerequisites . . . 36
Discovering an instrument . . . 37
About the Refresh key . . . 38
Sorting discovered instruments . . . 38
Observing details for an instrument . . . 39
Discovering network devices . . . 40
Programming JMEPs . . . 41
Protocol Analysis . . . 42

Layer 1 BER testing 43
BER testing layer 1 44
Monitoring layer 1 BER 45
Link connectivity testing 45
Layer 2 testing 46
Specifying interface settings 46
Specifying Ethernet frame settings 49
Things to consider 49
Specifying the settings 50
Configuring VLAN tagged traffic 54
Configuring Q-in-Q traffic 55
Configuring stacked VLAN traffic 55
Configuring VPLS traffic 55
Configuring LBM Traffic 56
Specifying Ethernet filter settings 56
Filtering traffic using Q-in-Q criteria 58
Filtering traffic using stacked VLAN criteria 59
Filtering traffic using VPLS criteria 60
Filtering traffic using MPLS criteria 61
Filtering traffic using byte pattern criteria 62
Filtering traffic using payload criteria 63
Specifying traffic load settings 64
Transmitting a constant load 64
Transmitting a bursty load 65
Transmitting a ramped load 67
Transmitting and analyzing layer 2 traffic 68
Transmitting and analyzing layer 2 patterns 69
Monitoring layer 2 traffic 70
Transmitting and analyzing layer 2 MPLS-TP, T-MPLS or MPLS traffic 70
About MPLS-TP 70
Transmitting and analyzing MPLS-TP traffic 71
Using J-Proof to verify layer 2 transparency 74
Understanding transparent loopbacks 75
Configuring the traffic originating instrument 75
Using Quick Config to configure test frames 76
Verifying the far end filter settings 77
Initiating the transparent loopback 77
Starting the frame sequence 78
Observing transparency results 78
Layer 3 testing 78
Specifying L3 interface settings 79
Specifying the data mode and link initialization settings 79
Configuring MPLS traffic 80
Specifying PPPoE settings 81
PPPoE messages 82
Terminating a PPPoE session 83
Specifying transmitted IPv4 packet settings 83
Specifying IPv4 filter settings 85
Specifying transmitted IPv6 packet settings 86
Specifying IPv6 filter settings 87
Transmitting and analyzing IP traffic 88

Ping testing . . . 89
Specifying IP settings for Ping and Traceroute testing . . . 90
Transmitting ping request packets . . . 91
Running Traceroute . . . 91
Monitoring IP traffic . . . 92
Capturing packets for analysis . . . 93
What is captured? . . . 93
Test traffic . . . 94
Control plane traffic . . . 94
How much can be stored in the buffer? . . . 94
Why use packet slicing? . . . 94
Understanding the Capture toolbar . . . 95
Specifying filter settings . . . 95
Capturing packets . . . 96
Manually capturing packets . . . 96
Capturing packets based on a trigger . . . 97
Saving or exporting captured packets . . . 100
How long will it take to save the PCAP file? . . . 101
Analyzing the packets using Wireshark® . . . 102
Analyzing the packets using J-Mentor . . . 103
Loop back testing . . . 105
Inserting errors or pause frames . . . 105
Inserting alarms or defects . . . 106
Measuring round trip delay or packet jitter . . . 106
Measuring one way delay . . . 107
CDMA/GPS receivers . . . 107
ATP-GPS test packets . . . 108
Network diagram . . . 108
Things to consider . . . 109
About the One Way Delay test option and accessory kit . . . 110
CDMA Receiver Kit . . . 110
GPS Receiver Kit . . . 110
Step 1: Connecting the receivers to your instruments . . . 111
Connecting the CDMA Receiver . . . 111
Connecting the GPS receiver . . . 112
Step 2: Measuring one way delay . . . 117
Measuring service disruption time . . . 118
OAM service and link layer testing . . . 119
Service layer features . . . 120
Link layer features . . . 120
Specifying OAM settings . . . 120
Turning AIS or RDI analysis ON . . . 125
Sending LBM or LTM messages . . . 125
MAC-in-MAC testing . . . 125
Understanding MAC-in-MAC test results . . . 125
Understanding the MAC-in-MAC LEDs . . . 126
Configuring layer 2 MAC-in-MAC tests . . . 126
Specifying interface settings . . . 126
Specifying Ethernet frame settings . . . 126
Specifying Ethernet filter settings for MiM traffic . . . 129
Specifying OAM settings . . . 130
Specifying traffic load settings . . . 130

Transmitting layer 2 MiM traffic . . . 130
Inserting errors or pause frames . . . 131
Measuring round trip delay and packet jitter . . . 131
Measuring service disruption time . . . 132
Monitoring layer 2 MiM traffic . . . 132
Synchronous Ethernet testing . . . 132
Transmitting and analyzing PTP/1588 traffic . . . 133
About PTP . . . 133
GPS as Time Source . . . 134
Connecting the GPS . . . 134
Configuring GPS as Source . . . 134
Analyzing PTP traffic . . . 134
Discovering traffic using J-Profiler . . . 136

Chapter 5 Wander Testing 139

About wander testing . . . 140
Features and capabilities . . . 140
Accessing wander test results . . . 140
Measuring and analyzing wander . . . 140
Measuring TIE and calculating MTIE . . . 141
SyncE Reference Timing Wander . . . 141
Analyzing wander . . . 142
Saving and exporting wander measurement data . . . 145

Chapter 6 TCP/UDP Testing 147

About TCP/UDP testing . . . 148
Features and capabilities . . . 148
Understanding the graphical user interface . . . 149
TCP/UDP test applications . . . 149
Understanding the ATP Listen IP and Port . . . 150
Specifying layer 2 and layer 3 settings . . . 152
Specifying layer 4 settings . . . 152
Well known ports . . . 153
Specifying TCP/UDP settings for transmitted traffic . . . 153
Configuring the traffic load . . . 154
Specifying the frame or packet length for transmitted traffic . . . 154
Filtering received traffic using layer 2 or layer 3 criteria . . . 155
Filtering received traffic using layer 4 criteria . . . 155
Transmitting layer 4 traffic . . . 157
Inserting errors or pause frames . . . 157
Loopback testing . . . 157
Running TCP Host or Wirespeed applications . . . 158
Changing settings during the test . . . 158
Streams pipe: multiple TCP streams . . . 158
Understanding the LED panel . . . 159
Understanding TCP Host and Wirespeed test results . . . 159
Viewing results for a specific stream . . . 159
Viewing cumulative link results . . . 159

Viewing TCP Host results . . . 159
Focusing on key results . . . 159
Configuring the streams . . . 160
Specifying TCP Host settings . . . 160
Running the TCP Host application . . . 162
Running the TCP Wirespeed application . . . 162
TrueSpeed . . . 164

Chapter 7 Triple Play and Multiple Streams Testing 165

About Triple Play and Multiple Streams testing . . . 166
Features and capabilities . . . 166
Streams Pipe soft key . . . 167
Using the action buttons . . . 167
Multiple Streams testing . . . 167
Multiple Streams test applications . . . 168
Understanding the LED panel . . . 169
Streams pipe: multiple streams . . . 169
Understanding multiple streams test results . . . 170
Viewing results for a specific stream . . . 170
Viewing cumulative link results . . . 170
Viewing graphical results for all streams . . . 170
Changing graph properties . . . 171
Enabling multiple streams . . . 172
Specifying the load type for all streams . . . 173
Specifying the load unit on a stream with burst . . . 174
Specifying the load unit for multiple streams . . . 175
Specifying common traffic characteristics for multiple streams . . . 175
Specifying layer 2 stream settings . . . 177
Automatically incrementing configured MAC addresses or VLAN IDs . . . 178
Specifying layer 3 stream settings . . . 179
Specifying layer 4 stream settings . . . 179
Transmitting multiple streams . . . 180
SAMComplete . . . 181
Triple Play testing . . . 181
Triple Play test applications . . . 181
Understanding the LED panel . . . 182
Streams pipe: Triple Play streams . . . 182
Understanding Triple Play test results . . . 183
Viewing cumulative link results . . . 183
Viewing graphs . . . 183
Changing graph properties . . . 183
Characterizing Triple Play services . . . 184
Specifying layer 2 and layer 3 settings for Triple Play services . . . 186
Transmitting multiple Triple Play streams . . . 186
Looping back multiple streams . . . 187
Running the TCP Host script . . . 187
Playing audio clips . . . 187

Chapter 8 Loop back Testing 189

About Loop back testing . . . 190
Loop back terminology . . . 190
Local unit . . . 190
Loop back unit . . . 190
Terminate mode . . . 190
Loop back mode . . . 190
Key loop back concepts . . . 191
ARP settings . . . 191
Address swapping . . . 191
Filter criteria on the loop back unit . . . 191
Loop types . . . 191
LBM Traffic . . . 192
VLAN and Q-in-Q traffic . . . 192
VPLS labels . . . 192
VPLS service provider and customer destination addresses . . . 192
MPLS labels . . . 192
MPLS destination addresses . . . 193
TCP/UDP ATP Listen IP Address and Listen Port . . . 193
Understanding the graphical user interface . . . 193
Loop back action buttons . . . 194
Loop back messages . . . 194
Loop back tests . . . 194
Specifying a unit identifier . . . 195
Using LLB to loop received traffic back to the local unit . . . 195
Using Loop Up to initiate a loop back from the local unit . . . 197

Chapter 9 IP Video Testing 201

About IP Video testing . . . 202
Understanding MPEG video transport streams . . . 202
Single program transport streams . . . 203
Multiple program transport streams . . . 203
Understanding the Explorer and Analyzer applications . . . 203
Explorer applications . . . 203
Analyzer applications . . . 203
Understanding MSTV . . . 204
Instant Channel Change (ICC) . . . 204
Microsoft R-UDP . . . 205
Features and capabilities . . . 205
Understanding the graphical user interface . . . 205
Action buttons . . . 206
Restart button . . . 206
Understanding the LED panel . . . 206
Understanding IP Video test results . . . 207
Layered view: Quality Layer Buttons . . . 207
Layered View: Button Colors . . . 208
Streams view . . . 210
Stream status icons . . . 211
Observing streams using the Explorer Application . . . 212
Observing streams using the Analyzer Application . . . 212
Static and dynamic test results . . . 213

Navigating the results display . . . 214
Customizing the results display . . . 214
IP Video test applications . . . 215
Populating the Address Book . . . 215
Adding streams . . . 215
Updating stream data . . . 216
Importing or exporting streams . . . 216
Specifying interface settings . . . 217
Specifying Video settings . . . 217
Specifying Ethernet filter settings . . . 217
Specifying result threshold settings . . . 219
Specifying latency distribution settings . . . 220
Specifying IGMP settings . . . 221
Joining streams . . . 222
Observing physical layer and link statistics . . . 223
Observing stream statistics . . . 224
Leaving streams . . . 224
Basic principles of IP Video testing . . . 225
IP Video network architecture . . . 225
MPEG-2 transport streams . . . 226
Packetized elementary streams (PES) . . . 226
Signaling tables . . . 226
IP Video encapsulation . . . 227
RTP . . . 227
Non-RTP . . . 227

Chapter 10 VoIP Testing 229

About VoIP testing . . . 230
Features and capabilities . . . 230
Understanding VoIP basics . . . 230
Understanding the graphical user interface . . . 231
Action buttons . . . 231
Understanding the LED panel . . . 232
Understanding the VoIP call bar . . . 232
Understanding VoIP test results . . . 232
Layered view: Quality Layer Buttons . . . 233
Layered View: Button Colors . . . 234
Navigating the results display . . . 235
VoIP test applications . . . 236
Populating the Address Book . . . 236
Specifying interface settings . . . 237
Specifying Ethernet frame and IP settings . . . 237
Specifying VoIP settings . . . 238
Specifying VoIP Filters . . . 241
Placing and receiving calls . . . 242
Registering with the server . . . 242
Placing calls . . . 243
Receiving calls manually . . . 243
Automatically answering calls . . . 244

Capturing packets for analysis 244
Understanding the Capture toolbar 244
Specifying filter settings 244
Capturing packets 245
Analyzing Audio Packets 246

Chapter 11 Fibre Channel Testing 247

About Fibre Channel Testing 248
Features and capabilities 248
Understanding the graphical user interface 249
Fibre Channel test applications 250
Configuring layer 1 tests 250
BER testing layer 1 250
Monitoring layer 1 BER 251
Configuring layer 2 Fibre Channel tests 252
Specifying interface settings 252
Specifying Fibre Channel frame settings 254
Specifying Fibre Channel filter settings 255
Specifying traffic load settings 256
Transmitting and analyzing layer 2 traffic 256
Loopback testing 257
Transmitting and analyzing patterns 257
Measuring service disruption time 258
Inserting errors 259
Measuring round trip delay 259
Monitoring layer 2 traffic 260
Emission Lowering Protocol 260

Chapter 12 Automated Testing 263

TrueSAM 264
Setting up TrueSAM 264
Loading TrueSAM Profiles 277
Running TrueSAM 278
Launching a single automated test 279
Automated Test Availability 281
Automated RFC 2544 and Fibre Channel tests 282
Features and capabilities 282
About loopbacks 283
J-QuickCheck 283
Understanding the J-QuickCheck stages 284
Test at configured Max Bandwidth 285
Layer 2 Quick Test 285
Asymmetrical tests 285
Throughput test 285
JDSU zeroing-in method 285
Throughput test results 286
Pass/fail threshold 287

Latency (RTD) test . . . 287
About the latency test . . . 287
Pass/fail threshold . . . 288
Packet Jitter test . . . 288
About the Packet Jitter test . . . 288
Packet Jitter test results . . . 288
Pass/fail threshold . . . 288
About the System Recovery test . . . 288
About the System Recovery test . . . 288
System Recovery test results . . . 289
Frame Loss test . . . 289
About the frame loss test . . . 289
Frame Loss test results . . . 289
Back to Back Frames test (Burst test) . . . 289
About the Back to Back Frames test . . . 289
Back to Back test results . . . 290
Optimizing the test time . . . 290
Importing and exporting RFC config files . . . 290
Initiating the Enhanced RFC2544 Test . . . 291
Configuring the Enhanced RFC 2544 or Fibre Channel tests . . . 291
Specifying the external test settings . . . 292
Setting Connection parameters . . . 293
Configuration methods . . . 293
Test selection . . . 296
Running Enhanced RFC 2544 and FC tests . . . 298
SAMComplete . . . 304
Initiating the SAMComplete test . . . 305
Configuring SAMComplete test settings . . . 306
Choosing SAMComplete tests . . . 314
Running SAMComplete tests . . . 314
Automated VLAN tests . . . 317
Automated FTP Throughput tests . . . 318
Automated HTTP Throughput tests . . . 320
Automated TCP Throughput tests . . . 321
TrueSpeed Test . . . 321
TrueSpeed test steps . . . 322
About the test steps . . . 322
Initiating the TrueSpeed test . . . 324
Configuring the TrueSpeed test . . . 324
Running the TrueSpeed test . . . 329
Testing using TAM automation . . . 332
Before testing . . . 333
Connecting to the management network . . . 333
Connecting to the test network . . . 334
Setting up a TAM test . . . 334
Saving automated test report data . . . 336

Chapter 13 Test Results 339

About test results. 340
Summary Status results 340
CPRI/OBSAI test results 341
CPRI and OBSAI LEDs 341
Interface/Signal results 342
CPRI/OBSAI Error Stats 343
CPRI/OBSAI Counts results 343
CPRI L1 Inband Protocol results 344
OBSAI Status Results 344
CPRI/OBSAI Payload BERT results 345
Ethernet, IP, TCP/UDP, and Fibre Channel results 345
Ethernet, IP, TCP/UDP, and Fibre Channel LEDs 347
Cable Diagnostic results 351
MDI or MDIX Status result 351
Fault Type result 352
Distance (m) result 353
Skew (ns) result 353
Polarity result 353
Pair result 353
SLA/KPI 353
Interface results 354
L2 Link Stats results 355
L2 Link Counts results 359
L2 Filter Stats results 361
L2 Filter Counts results 365
J-Proof (transparency) results 366
L2 BERT Stats results 367
CDMA Receiver Status results 368
CDMA/GPS Receiver Log 368
Ethernet OAM Service OAM results 369
Ethernet OAM Service OAM MEP Discovery results. 371
Ethernet OAM L-OAM Modes results 371
Ethernet OAM L-OAM Counts results 372
Ethernet OAM L-OAM States results. 373
Ethernet OAM L-OAM Error History results. 373
L3 Link Stats results 374
L3 Link Counts results 375
L3 Filter Stats results 376
L3 Filter Counts results 377
L3/IP Config Status results 377
Ping results 378
Traceroute results 379
PCS Error Stats 379
Ethernet Per Lane results 380
Error Stats results 381
Error Stats (Layer 1 BERT) 381
Error Stats (Layer 2 Traffic) 383
Error Stats (Layer 3 Traffic) 384
Capture results 385
Sync Status Messages 386

AutoNeg Status results . . . 386
Login Status results . . . 388
Implicit or Explicit (E-Port) login . . . 388
Explicit (Fabric/N-Port) login . . . 388
PTP Link Counts results . . . 390
PTP Link Stats results . . . 391
PTP Graphs . . . 393
L4 Link Stats results . . . 393
Detailed L4 Stats . . . 393
Cumulative L4 results . . . 394
L4 Link Counts results . . . 395
L4 Filter Stats results . . . 395
L4 Filter Counts results . . . 395
J-Profiler results . . . 395
Wander Interface results . . . 396
IP Video results . . . 397
IP Video LEDs . . . 398
Physical/Link Stats results . . . 399
All Streams Transport results . . . 400
All Streams Video/All Program Video results . . . 403
All Streams Complete results . . . 405
Individual stream results . . . 406
Stream and Program PID results . . . 406
MSTV results . . . 407
MSTV Stats . . . 407
MSTV Count . . . 407
MSTV Latency Distribution . . . 407
MSTV Message Log . . . 408
VoIP results . . . 408
VoIP LEDs . . . 408
Content results . . . 409
Transport results . . . 410
QoS results . . . 410
Stats/Counts results . . . 411
Transaction Log results . . . 411
Miscellaneous measurements . . . 411
Measurement results . . . 412
Call Stats results . . . 412
Ethernet results . . . 413
Stats results . . . 413
Capture results . . . 413
Auto Neg Status . . . 413
Graph results . . . 413
Graphical results . . . 413
Histogram results . . . 414
Event Log results . . . 414
Time test results . . . 415

Chapter 14 Troubleshooting 417

Before testing 418
The test application I need is not available 418
Can I hot-swap PIMs? 418
How can I determine whether I need to swap a PIM or swap SFP transceivers? 418
I am receiving unexpected errors when running optical applications 418

Performing tests 418
Optical Overload Protection message 418
User interface is not launching 419
Inconsistent test results 419
Result values are blank 419
Unit on far end will not loop up 419
A receiving instrument is showing many bit errors 419
RFC 2544 or FC Script button does not appear 420
Which MSAM or application module is selected? 420
I am transmitting Layer 2 Ethernet traffic with OAM frames at 10 Mbps, but no frames are transmitted or received 420
One way delay measurements do not appear 420
My VoIP call didn't go through 421
I am emulating a SIP phone but cannot register with the SIP server 421
I am running a VoIP test but the delay measurement does not appear 422
I have very little loss, but a high level of delay on my VoIP test 422
I have a large amount of jitter in my VoIP test, but no loss or delay 422

Upgrades and options 422
How do I upgrade my instrument? 422
How do I install test options? 422
Do software and test options move with the Dual Module Carrier, Transport Module, and MSAM or Transport Module? 422

Glossary 423

Index 433

About this Manual

This prefix explains how to use this manual. Topics discussed include the following:

– “Purpose and scope” on page xx
– “Assumptions” on page xx
– “Terminology” on page xx
– “Ethernet, IP, TCP/UDP, Fibre Channel, and IP Video Testing Manual” on page xxii
– “Conventions” on page xxiii
– “Safety and compliance information” on page xxiv
– “Technical assistance” on page xxiv

Purpose and scope

The purpose of this manual is to help you successfully use the Ethernet, IP, TCP/UDP, Fibre Channel, and IP Video test capabilities of the Dual Module Carrier, 40G/100G High Speed Transport Module, and MSAM for the T-BERD/MTS 8000 and T-BERD/MTS 6000A platforms as well as each of the members of the T-BERD/MTS 5800 Handheld Network Test Family.

This manual includes task-based instructions that describe how to configure, use, and troubleshoot the general functions of your instrument.

Assumptions

This manual is intended for novice, intermediate, and experienced users who want to use the 40G/100G High Speed Transport Module, Transport Module, Multiple Services Application Module, or 5800 effectively and efficiently. We are assuming that you have basic computer experience and are familiar with basic telecommunication concepts, terminology, and safety.

Terminology

The T-BERD 8000 is branded as the MTS-8000 in Europe, and it is interchangeably referred to as the T-BERD 8000, MTS 8000, MTS-8000, MTS8000 and Media Test Set 8000 throughout supporting documentation.

The T-BERD 6000A is branded as the MTS-6000A in Europe, and it is interchangeably referred to as the T-BERD 6000A, MTS 6000A, MTS6000A and Media Test Set 6000 throughout supporting documentation.

The T-BERD 5800 is branded as the MTS-5800 in Europe, and it is interchangeably referred to as the T-BERD 5800, MTS 5800, MTS-5800, MTS5800 and Media Test Set 5800 throughout supporting documentation.

The following terms have a specific meaning when they are used in this manual:

- **Assembly** — Used throughout this manual to refer to a complete *set of components* assembled as an instrument and used for testing. This manual supports three assemblies:
  - ***40/100G Transport Module assembly***, consisting of an T-BERD/MTS 8000 base unit and 40/100G Transport Module
  - ***CSAM assembly***, consisting of a CSAM and either a DMCv2 or 6000Av2 base unit.
  - ***MSAM assembly***, consisting of a MSAM, Physical Interface Modules (PIMs), and a T-BERD/MTS 6000A base unit
  - ***DMC assembly***, consisting of up to two MSAMs, up to four PIMs, a Dual Module Carrier (DMC), and a T-BERD/MTS 8000 base unit.
- **Application module**—Used throughout this manual to refer to the component that provides test functionality to the assembled instrument. This manual supports two application modules: the ***Transport Module***, and the ***MSAM***.
- **Component**—Used throughout this manual to refer to an individual hardware *component* which is connected to the other components to build a test instrument (assembly). This manual supports the following components: the Transport Module, the MSAM, and the DMC. The base units are documented in separate manuals.

- **T-BERD / MTS 8000, 6000A, and 5800**—The family of products, typically a combination of a base unit, a battery module, and one or more application modules. The Dual Module Carrier (DMC) can be used on the T-BERD / MTS 8000 platform to test using two MSAMs.
- **Base unit**—The unit which connects to the application module and power adapter, providing the user interface and a variety of connectivity and work flow tools. If optioned to do so, the base unit also allows you to measure emitted power, received power, and optical link loss on fiber optic networks.
- **CSAM 100G Services Application Module**—Referred to generically as “the instrument” when inserted in the T-BERD / MTS 6000A base unit or the DMC with a PIM. The CSAM provides testing functionality for the base unit.
- **DMC**—Dual Module Carrier. The DMC is a two slot chassis which you can connect to the T-BERD / MTS 8000 base unit to test using up to two MSAM application modules and four Physical Interface Modules (PIMs).
- **MSAM Multiple Services Application Module**—Referred to generically as “the instrument” when inserted in the T-BERD / MTS 6000A base unit or the DMC with a PIM. The MSAM provides testing functionality for the base unit.
- **Transport Module**—Referred to generically as “the instrument” when connected to the T-BERD / MTS 8000 base unit. The Transport Module provides testing functionality for the base unit.
- **PIM—**The physical interface module inserted into one of up to two ports provided on the MSAM chassis. PIMs supply the physical connectors (interfaces) required to connect the MSAM to the circuit under test. A variety of cables, SFPs, and XFPs are offered as options, and can used to connect the PIMs to the circuit.
- **Battery Module—**The module connected to the back of the T-BERD / MTS 8000 base unit, which supplies power whenever it is not provided using the power adapter.
- **OC-n**—Used to refer to each of the optical SONET rates supported by the instrument (OC-3, OC-12, OC-48, and OC-192), where *“n”* represents the user-selected line rate.
- **STM-n**—Used to refer to each of the optical SDH rates supported by the instrument (STM-1, STM-4, STM-16, and STM-64), where *“n”* represents the user-selected line rate.
- **STS-1**—Used to refer to the electrical equivalent of OC-1 (51.84 Mbps) supported by the instrument.
- **STM-1e**—Used to refer to the electrical equivalent of STM-1 (155.52 Mbps) supported by the Dual Module Carrier, Transport Module, and MSAM.
- **OTN**—Optical Transport Network.
- **OTU1**—Optical Transport Unit 1. A 2.7G OTN signal designed to carry a SONET OC-48 or SDH STM-16 client signal. OTU1 is used on the user interface to identify the applications used for 2.7G OTN testing.
- **OTU2**—Optical Transport Unit 2. A 10.7G, 11.05G, or 11.1G OTN signal designed to carry SONET OC-192, SDH STM-64, or 10GigE Ethernet WAN and LAN client signals. OTU2 is used on the user interface to identify the applications used for 10.7G, 11.05G, or 11.1G OTN testing.
- **OTU3** — Optical Transport Unit 3. A 43G OTN signal designed to carry 40GigE BERT signals. OTU3 is available on the 40G/100G High Speed Transport Module.
- **OTU4** — Optical Transport Unit 4. A 111.8G OTN signal designed to carry 100GigE Ethernet BERT and ODU4 encoded signals. OTU4 is available on the 40G/100G High Speed Transport Module.
- **1GigE**—Used to represent 1 Gigabit Ethernet.
- **10GigE**—Used to represent 10 Gigabit Ethernet.
- **40GigE** — Used to represent 40 Gigabit Ethernet.
- **100GigE** — Used to represent 100 Gigabit Ethernet.

- **FC**—Used to represent Fibre Channel.
- **JDSU Ethernet test set**—A test set marketed by JDSU and designed to transmit an Acterna Test Packet (ATP) payload. ATP packets carry a time stamp used to calculate a variety of test results. The FST-2802 TestPad, the SmartClass Ethernet tester, the HST with an Ethernet SIM, the T-BERD/MTS 8000 Transport Module, and the MSAM can all be configured to transmit and analyze ATP payloads, and can be used in end-to-end and loopback configurations during testing.
- **SFP**—Small Form-factor Pluggable module. Used throughout this manual to represent pluggable optical modules.
- **XFP**—10 Gigabit small form-factor pluggable module. Used throughout this manual to represent pluggable optical modules used to connect to the family of 10 Gbps circuits (ranging from 9.95 Gbps to 11.3 Gbps).
- **QSFP+** — Quad Small Form-Factor Pluggable optical transceiver. A variety of optional QSFP+s are available for testing 40 Gigabit fiber circuits.
- **CFP** — C Form-Factor Pluggable optical transceiver. A variety of optional CFPs are available for testing 100Gigabit fiber circuits.
- **Xv**—Used as a suffix throughout the user interface for virtual channels carried in a SONET or SDH container, where X serves as a placeholder for the number of virtual channels, and “v” indicates that the concatenation is virtual (rather than true concatenation). For example, if you are testing virtual channels carried in a high order STS-3c, you would select an STS-3c-Xv payload when you launched your application. You can then specify the number of members (channels) when you create the virtual channel group (VCG).

Ethernet, IP, TCP/UDP, Fibre Channel, and IP Video Testing Manual

This is the Ethernet, IP, TCP/UDP, Fibre Channel, and IP Video testing manual for the T-BERD⁄MTS 5800, MSAM and the Transport Module. The manual is application-oriented and contains information about using these instruments to test service carried on each of the listed networks. It includes an overview of testing features, instructions for using the instruments to generate and transmit traffic over a circuit, and detailed test result descriptions. This manual also provides contact information for JDSU’s Technical Assistance Center (TAC).

Use this manual in conjunction with the following manuals:

- *8000 Base Unit User Manual*. This manual provides an overview, specifications, and instructions for proper operation of the base unit (The 40G/100G High Speed Transport Module requires the 8000E Base Unit).
- *6000A Base Unit User Manual*. This manual provides an overview, specifications, and instructions for proper operation of the base unit.
- *Dual Module Carrier, Transport Module, and Dual Module Carrier, Transport Module, and MSAM Getting Started Manual.* This manual provides an overview of the connectors provided on the hardware components, instructions for connecting to the circuit you are testing, and specifications for the hardware components.
- *PDH, SONET, SDH, NextGen, and OTN Testing Manual*. This manual provides instructions for testing each of the services listed, and detailed test result descriptions. When using your instrument for NextGen and OTN testing, details concerning SONET and SDH settings and test results are provided in this manual.

– *Remote Control Reference Manual*. This manual provides the remote control commands used when developing scripts to automate your testing. This manual is provided electronically on the USB stick.



NOTE:

Many applications also require you to purchase and install certain testing options; others require specific hardware connectors to connect to circuits for testing. For example, if your instrument does not have a connector or PIM designed to support 1GigE Optical testing, you can not transmit and analyze a signal or traffic over a 1GigE circuit.

You can quickly determine whether or not your instrument supports certain applications by exploring the technologies, rates, and test modes presented on the Test menu and by reviewing the settings available when you configure a test.

Conventions

This manual uses conventions and symbols, as described in the following tables.

Table 1 Typographical conventions

Description	Example
User interface actions and buttons or switches you have to press appear in this **typeface**.	Press the **OK** key.
Code and output messages appear in this `typeface`.	`All results okay`
Text you must type exactly as shown appears in this **`typeface`**.	Type: **`a:\set.exe`** in the dialog box.
Variables appear in this ***typeface***.	Type the new ***hostname***.
Book references appear in this *typeface*.	Refer to *Newton's Telecom Dictionary*

Table 2 Keyboard and menu conventions

Description	Example
A plus sign +indicates simultaneous keystrokes.	Press **Ctrl+s**
A comma indicates consecutive key strokes.	Press **Alt+f,s**
A slanted bracket indicates choosing a submenu from menu.	On the menu bar, click **Start > Program Files**.

Table 3 Symbol conventions



This symbol represents a general hazard.



This symbol represents a risk of electrical shock.



This symbol represents a risk of explosion.



This symbol represents a Note indicating related information or tip.



This symbol, located on the equipment, battery, or packaging indicates that the equipment or battery must not be disposed of in a land-fill site or as municipal waste, and should be disposed of according to your national regulations.

Safety and compliance information

Safety and compliance information for the instrument are provided in printed form and ship with your instrument.

Technical assistance

Table 4 lists contact information for technical assistance. For the latest TAC information, go to www.jdsu.com or contact your local sales office for assistance. Contact information for regional sales headquarters is listed on the back cover of this manual.

Table 4 Technical assistance centers

Region	Phone Number	
Americas	1-855-ASK-JDSU (option #3) 301-353-1560	(1-855-275-5378, option #3) tac@jdsu.com
Europe, Africa, and Mid-East	+49 (0) 7121 86 1345 (JDSU Germany)	hotline.europe@jdsu.com
Asia and the Pacific	+852 2892 0990 (Hong Kong) +86 10 6655 5988 (Beijing-China)	

During off-hours, you can request assistance by doing one of the following: leave a voice mail message at the Technical Assistance number, e-mail the North American Technical Assistance Center, tac@jdsu.com, or submit your question using our online Technical Assistance Request form at www.jdsu.com.

1

Basic Testing

This chapter explains basic testing concepts and procedures common to each Ethernet, IP, TCP/UDP, Fibre Channel, or IP Video test. Detailed information about concepts and procedures shared by all supported test applications are provided in the Getting Started manual that shipped with your instrument or upgrade,

Topics discussed in this chapter include the following:

– “Step 1: Selecting a test application” on page 2
– “Step 2: Configuring a test” on page 2
– “Step 3: Connecting the instrument to the circuit” on page 3
– “Step 4: Starting the test” on page 3
– “Step 5: Viewing test results” on page 4
– “Running multiple tests” on page 5

Step 1: Selecting a test application

The Test menu on the Main screen lists each of the available test applications.

If you are testing using an MSAM, the applications are listed for the PIM or PIMs that are inserted in your Transport Module chassis. If you have a dual port chassis, by default, the first application you select will be for port 1 (P1).

To select an application

Step1 Select **Test**. The Test menu appears.

Step2 Select the technology (for example, Ethernet), signal, payload, and test mode for your test application.

The instrument displays a message asking you to wait while it loads the application.

Step3 Wait for the Main screen to appear, and then proceed to "Step 2: Configuring a test" on page 2.

The test application is selected.



NOTES:

When testing using an MSAM, only the applications for currently inserted PIMs will appear on the Test menu. For example, if an SFP and XFP PIM are inserted in the Transport Module chassis, you will not see DS1 applications.

When testing using a T-BERD/MTS 5800, only the applications for currently inserted SFPs will appear on the Test menu. For example, if you do not have a 5800 chassis that supports PDH you will not see selectable test options for PDH.

Other applications, such as the Mac-in-Mac or NextGen GFP applications only appear if you purchased the associated testing options.

Step 2: Configuring a test

Before you configure a test, be certain to complete the information that you want to include when you generate reports of your test results. For details, refer to the Getting Started manual that shipped with your instrument.

Configuring a test involves displaying the setup screens, specifying test settings, and optionally saving the test setup. Key settings are also available on the Main screen, on the Quick Config tabs. Changing key settings while running a test (for example, changing the pattern transmitted) triggers an automatic restart of the test.

To display the setup screens

Step1 Using the Test menu, select a test application (see "Step 1: Selecting a test application" on page 2).

Step2 Select the **Setup** soft key.

A setup screen with a series of tabs appears. The tabs displayed vary based on the test application you selected.

Step3 To navigate to a different setup screen, select the corresponding tab at the top of the screen. For example, to display the Traffic setup screen, select the Traffic tab.

Step 3: Connecting the instrument to the circuit

For detailed instructions on connecting your instrument to the circuit, refer to the Getting Started Manual.

When connecting the unit to optical circuits, bear in mind that applied power must not exceed the power level specified on the panel for each optical connector.

Step 4: Starting the test

After you configure a test, connect the unit to the circuit, and, if appropriate, turn the laser ON.

- If you are running an Ethernet, OTN, Fibre Channel, or NextGen application (launched from the SONET or SDH test menu options), you must turn the laser ON (if you are testing an optical circuit), and then actively **Start Traffic** (using the action button).
- If you are running an Ethernet or Fibre Channel application, and you would like your unit to transmit traffic automatically, you can enable the automatic traffic generation feature. For details, see “Enabling automatic traffic transmission” on page 35 in Chapter 4 “Ethernet and IP Testing”.
- When a test is configured to establish a connection to a remote unit, the connection process queries the remote unit for its software version. If the version level of the remote and local unit are different, a notice will be displayed encouraging the user to update the older unit to avoid incompatibility issues and to achieve optimal performance. See “Setting up the Instrument” in the *Getting Started Manual* that shipped with this unit.



NOTE: Temperature stabilized lasers

When testing 10 Gigabit, 40 Gigabit or 100Gigabit optical circuits, some lasers (particularly 1550 nm lasers) are temperature stabilized; therefore, they need to reach a certain temperature before you can use them to transmit a signal. This is expected behavior, and does not indicate that there is something wrong with the laser or test instrument.

It typically takes up to one minute for the temperature to stabilize. If you have turned the laser on, but no signal is present on the receiving instrument or device, simply wait for one minute.

After you start a test, use the buttons at the bottom of the screen to perform actions such as turning the laser on and off, starting and stopping traffic, starting and stopping a local loop back, and inserting errors, anomalies, alarms, or defects. Table 1 lists some common Action buttons.

Table 1 Action buttons

Button	Action
Laser On/Off[a]	Turns the laser on or off when testing optical rates.
Insert Error/Anomaly	Inserts an error or anomaly into the transmitted traffic.
Insert Alarm/Defect	Inserts an alarm or defect into the transmitted traffic.
Start Traffic/Stop Traffic	Starts or stops transmission of Ethernet, IP, Fibre Channel, OTN, TCP/UDP, or GFP traffic over the circuit.

a. You can optionally configure optical standard Ethernet and Fibre Channel applications to automatically transmit traffic after you turn the laser ON.

Step 5: Viewing test results

Test results appear in the Results Windows of the Main screen.

Setting the result group and category

To set the result group and category

Step1 Using the Test menu, select a test application see “Step 1: Selecting a test application” on page 2), and then configure your test (see “Step 2: Configuring a test” on page 2).

Step2 Select the **Results** soft key to return to the Main screen.

Step3 Connect your module to the circuit (see “Step 3: Connecting the instrument to the circuit” on page 3).

Step4 If you are testing an optical interface, select the **Laser** button.

Step5 If you selected an Ethernet, Fibre Channel, or SONET/SDH GFP test application, select the **Start Traffic** button to start generating and analyzing traffic.

Results appear in the Results Windows.

Step6 *Optional*. Insert errors or anomalies into the traffic stream, or use the Action buttons to perform other actions. These buttons only appear if applicable to your test application.

Step7 Use the Group and Category buttons to specify the type of results you want to observe. Figure 1 illustrates buttons for a standard Ethernet application.

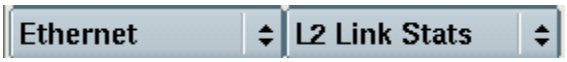


Figure 1 Result Group and Category buttons

Results for the category you selected appear in the result window.

Step8 *Optional*. To observe results for a different group or category in another result window, press the buttons at the top of the window to specify the group and category.

For descriptions of each result, refer to Chapter 13 “Test Results”.

TIP:

If you want to provide a screen shot of key test results, on the Main screen, select **Tools > Capture Screenshot**. A screen shot will be captured and stored as a JPG file in the `/acterna/user/disk/bert/images` folder. You can include the screen shot when you create reports.

Additional test result information

For detailed information on the following topics, refer to the Getting Started manual that shipped with your instrument or upgrade.

– Expanding and collapsing result measurements
– Changing the result layout
– Using the entire screen for results
– About histogram results

– Viewing a histogram
– About the Event log
– About result graphs
– Clearing History results
– Creating and maintaining Custom result groups

For descriptions of each result, refer to Chapter 13 “Test Results”.

Running multiple tests

You can significantly reduce your testing time by terminating traffic over multiple circuits simultaneously.

For example, if your instrument is configured and optioned to do so, you can transmit traffic from the SFP and XFP PIMs to a network element, and then loop the traffic back to your unit to analyze the signals and verify that the network element is operating properly.

In addition, you can display two test result windows side-by-side using the Dual Test View button.

For details, refer to the Getting Started manual that shipped with your instrument or upgrade.

2

Optical BERT Testing

This chapter provides information on testing Optical BERT services using the MSAM. Topics discussed in this chapter include the following:

– “About Optical BERT testing” on page 8
– “BER Testing Optical Layer 1” on page 8
– “Monitoring Optical Layer 1” on page 9

About Optical BERT testing

The Optical BERT test is used to validate that the underlying dark fiber/DWDM network is configured correctly to support 3072.0M (3.072G) or 9830.4M protocol without errors.

If your instrument is equipped with the option, it supports both Terminate and Monitor modes.

BER Testing Optical Layer 1

To BER test Optical Layer1

Step1 Using the Test Menu, select the Optical BERT 3072.0M or 9830.4M Optical Layer 1 BERT Terminate application.

Step2 To specify the BER pattern, do the following:

a Select the **Setup** soft key, and then the Pattern tab.

b Select a pattern.

Pattern	Description
2^23-1 ANSI	Selects the 2^{23} -1 pseudorandom pattern, which generates a maximum of 22 sequential 0s and 23 sequential 1s. Usually used to simulate live data for DS3 and SONET circuits.
2^23-1 Inv ANSI	Selects the inverted 2^{23} -1 pseudorandom pattern, which generates a maximum of 22 sequential 1s and 23 sequential 0s. Usually used to simulate live data for DS3 and SONET circuits.
Delay	2^{23}-1 PRBS with multi-Bit Error Insertion for Latency Measurement. This is an unframed Layer 1 Pattern. This pattern delivers energy across the entire frequency spectrum delivering a good basic Bit Error Test for the optical transmission line. The periodic insertion of multiple bit errors permit a high-accuracy measurement of timing in the 100s of nanoseconds range.

To measure round trip delay, use the **Delay** pattern.



NOTE:

There must be a loop at the far end (hard cable/fiber loop or far end test set in Mon application with Rx = Tx selected) to measure round trip delay.

c Specify whether to link the Rx pattern to the Tx pattern.

d If you did *not* link the Rx pattern to the Tx pattern, specify the **Rx pattern**.

e Press **Results** to return to the Main screen.

Step3 Connect the module to the circuit.

Step4 Select the **Laser** button.

Step5 Verify that the green Signal LED is illuminated.

Step6 If desired, specify the error insertion parameters at the bottom of the page and press the **Error Insert** button to insert into the signal.

Step7 Observe the test results in the following categories:

– Interface Signal - Stats such as *Signal-Losses* and *Loss Seconds; Rx, Optical-Overload* and *Level; Frequency* and *Clock Specs*

– 3.072G Optical BERT- Error Stats such as *Pattern Sync Losses* and *Pattern Sync Loss Seconds* (all)*, Bit Error Rate, Errors* and *Seconds* (typical BERT patterns), or *Round Trip Delay (*Delay pattern).

3.072G Optical Layer 1 BERT is complete

Monitoring Optical Layer 1

To monitor Optical Layer1

Step1 Using the Test Menu, select the Optical BERT 3072.0M or 9830.4M Optical Layer 1 BERT Monitor/Thru application.

Step2 To specify the BER pattern, do the following:

a Select the **Setup** soft key, and then the Pattern tab.

b Specify the **Rx Pattern**.

To monitor round trip delay, use the **Delay** pattern.



NOTE:

The Rx Pattern selection specifies which pattern to analyze, it does not change the transmit data from the terminating unit.

c Press **Results** to return to the Main screen.

Step3 Connect the module to the circuit.

Step4 If you are testing an optical interface, select the **Laser** button.

Step5 Verify that the green Signal LED is illuminated.

Step6 Press the **Restart** soft key.

Step7 Observe the test results in the following categories:

– Interface Signal - Stats such as *Signal-Losses* and *Loss Seconds; Rx, Optical-Overload* and *Level; Frequency* and *Clock Specs*

– 3.072G Optical BERT- Error Stats such as *Pattern Sync Losses* and *Pattern Sync Loss Seconds* (all)*, Bit Error Rate, Errors* and *Seconds* (typical BERT patterns), or *Round Trip Delay (*Delay pattern).

You are monitoring Optical layer 1.

3

CPRI/OBSAI Testing

This chapter provides information on testing CPRI services using the MSAM. Topics discussed in this chapter include the following:

– “About CPRI/OBSAI testing” on page 12
– “Layer 1 CPRI or OBSAI BER Testing” on page 12
– “Layer 2 CPRI testing” on page 15
– “Layer 2 OBSAI testing” on page 16
– “Inserting errors” on page 18
– “Monitoring CPRI or OBSAI layer 1” on page 18

About CPRI/OBSAI testing

Common Public Radio Interface (CPRI) protocol is used on 3G/4G wireless network deployments to implement a more cost effective distributive wireless base station architecture. CPRI is the communication protocol used to synchronize, control, and transport data between the radio controller and remote radio heads. The CPRI test is used to validate that the underlying dark fiber/ DWDM network is configured correctly for these new rates and meet CPRI service requirements.

Open Base Station Architecture Initiative Reference Point 3 (OBSAI RP3) refers to the interface between the baseband and RF components within a cellular base station. The OBSAI test is used to verify the CWDM links between the Central Office and the base station.

CPRI Layer 2 testing enables field technicians to verify that fiber installation is correctly performed and CPRI Link is functional before the Radio Equipment Controller at the central office is installed and connected to the overall system.

NOTE:
CPRI /OBSAI testing is only applicable to 8000 UIMv2 or higher.

Layer 1 CPRI or OBSAI BER Testing

If your instrument is optioned to do so, you can BERT over CPRI or OBSAI.

NOTE
614.4M and 1228.8M CPRI along with 768M and 1536M OBSAI are the only rates available on MSAMv1.

To BER test CPRI or OBSAI

Step1 Using the Test Menu, select the CPRI or OBSAI Layer 1 BERT Terminate application.

Protocol	Frequency	Layer 1 BERT Applications
CPRI	614.4M[a]	P1 Terminate P2 Terminate
	1228.8M[a]	P1 Terminate P2 Terminate
	2457.6M[a]	P1 Terminate P2 Terminate
	3072.0M[a]	P1 Terminate P2 Terminate
	4915.2M	P1 Terminate P2 Terminate
	6144.0M	P1 Terminate P2 Terminate
	9830.4M	P1 Terminate P2 Terminate

Protocol	Frequency	Layer 1 BERT Applications
OBSAI	768M[a]	P1 Terminate P2 Terminate
	1536M[a]	P1 Terminate P2 Terminate
	3072.0M[a]	P1 Terminate P2 Terminate
	6144.0M	P1 Terminate P2 Terminate

a. Available on MSAM v1.

NOTE:
You must use a XFP if testing CPRI at 9.8G, or a SPF+ for 4.9G and 6.1G.

Step2 To specify the BER pattern, do the following:

a Select the **Setup** soft key, and then the Pattern tab.

b Select a pattern.

Pattern	Description
2^23-1 ANSI	Selects the 2^{23} -1 pseudorandom pattern, which generates a maximum of 22 sequential 0s and 23 sequential 1s. Usually used to simulate live data for DS3 and SONET circuits.
2^23-1 Inv ANSI	Selects the inverted 2^{23} -1 pseudorandom pattern, which generates a maximum of 22 sequential 1s and 23 sequential 0s. Usually used to simulate live data for DS3 and SONET circuits.
Delay	2^{23}-1 PRBS with multi-Bit Error Insertion for Latency Measurement. This is an unframed Layer 1 Pattern. This pattern delivers energy across the entire frequency spectrum delivering a good basic Bit Error Test for the optical transmission line. The periodic insertion of multiple bit errors permit a high-accuracy measurement of timing in the 100s of nanoseconds range.
Test Patterns	Includes: – D6.6 D25.6 – 2^23-1 ANSI – 2^23-1 Inv ANSI – Delay – 2^31-1 (only available for 9.8G test) – 2^31-1 Inv (only available for 9.8G test)

These patterns are formatted using the 8B/10B symbol framing format. This allows these patterns to be passed by network elements that require basic synchronization messages as built into 8B/10B framing. These patterns are therefore intended to confirm the ability of the Physical Coding Sub-layer (PCS) of equipment that implements 8B/10B to properly synchronize to another element under specific conditions.

Figure 2 through Figure 4 show the details of the specific 8B/10B Encoded test patterns for CPRI and OBSAI used to verify the correct operation of the RF/Baseband interface. The Pseudo-Random Bit Sequence (PRBS) will be inserted as shown in Figure 4 on page 14.

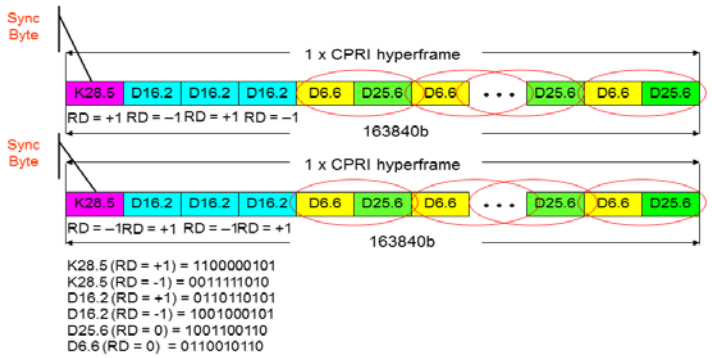


Figure 2 Test pattern (D6.6 D25.6) frame for CPRI

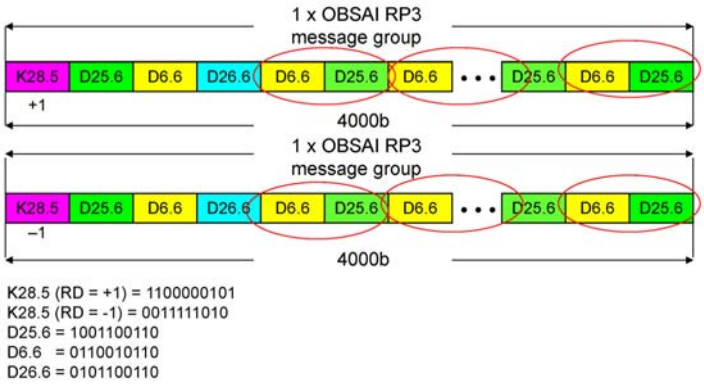


Figure 3 Test pattern (D6.6 D25.6) frames for OBSAI

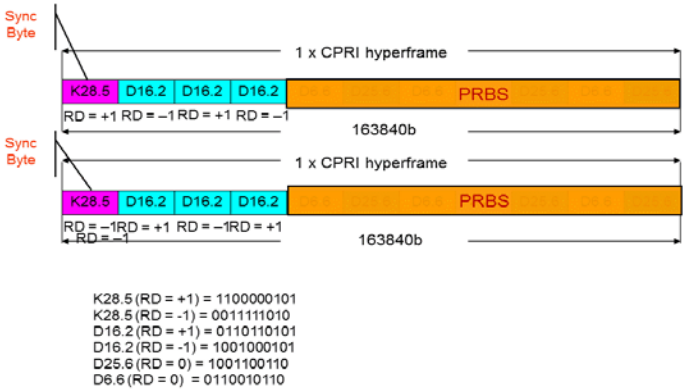


Figure 4 Test pattern (PRBS) frames for CPRI

To measure round trip delay, use the **Delay** pattern. NOTE: There must be a loop at the far end (hard cable/fiber loop or far end test set in Mon application with Rx = Tx selected) to measure round trip delay.

c Specify whether to link the Rx pattern to the Tx pattern.

d Select the **Tx Pattern.** If you did *not* link the Rx pattern to the Tx pattern, also specify the **Rx pattern**.

e Select the **Payload Analysis** checkbox if you'd like to see pattern sync, bit errors, etc. reported in the Results.

f Press **Results** to return to the Main screen.

Step3 Connect the module to the circuit. Select either **SFP1** or **SFP2.**

Step4 If you are testing an optical interface, select the **Laser** button.

Step5 If the Tx Frequency needs to be offset, select the **Actions** tab at the bottom of the page and then select the **Offset Tx Freq** button. This will activate the available offset frequency options. Select the desired offset.

Step6 To insert errors into the transmission, select the **Error** tab at the bottom of the page and then select from the available **Error Types**, **Insertion Types** and insertion **Rates**. Press the **Insert Error** button to initiate error insertion.

Step7 Press the **Start BERT Pattern** action button to start inserting the BERT pattern.

This button appears when using the typical BERT patterns; it does not apply if you are using the Delay pattern.

Step8 Verify that the green Signal LED is illuminated.

CPRI/OBSAI layer 1 BERT is complete.

Layer 2 CPRI testing

If your instrument is optioned to do so, you can set Overhead Bytes, configure a payload and perform BER testing (with optional alarm insertion) of your CPRI circuit.

NOTE:

CPRI Layer 2 testing is not applicable to MSAMv1 or T-BERD/ MTS 8000v1 DMC.

CPRI Layer 2 testing at 4915.2M and 6144.0 rate is not available on T-BERD 5800.

To configure Layer 2 CPRI testing

Step1 Using the Test Menu, select a CPRI Layer 2 BERT Terminate application.

Protocol	Frequency	Applications
CPRI	614.4M	Layer 2 BERT Terminate
	1228.8M	Layer 2 BERT Terminate
	2457.6M	Layer 2 BERT Terminate
	3072.0M	Layer 2 BERTTerminate
	4915.2M	Layer 2 BERTTerminate
	6144.0M	Layer 2 BERTTerminate

Step2 Select the **Setup** soft key, and then the CPRI tab.

a Define the **Port Type** and **Start-Up Sequence**.

b If the Start-Up Sequence is Bypass, specify the Protocol version.

c Specify the Control and Management parameters, if necessary.

– HDLC rate (or No HDLC).
– Whether the Ethernet Channel is enabled.
– If the Ethernet Channel is enabled, enter the Ethernet Sub-channel Number.

Step3 Select the **Pattern** tab.

a Select a Pattern Mode.

b Select the desired pattern from the list of available patterns.

Step4 If service disruption detection is desired, select the **Service Disruption** tab and click the Enable checkbox. Define the parameters to be detected from the available selections.

Step5 If a timed or delayed start test is required, select the **Timed Test** tab and specify the desired start times and duration.

Step6 Select the **Results** soft key to return to the Main screen.

Step7 Select the Laser Tab at the bottom of the screen and click the **Laser On** button.

Step8 Select the CPRI result group and then choose a category to view:

– Error Stats
– Counts
– L1 Inband Protocol

You are testing CPRI layer 2.

Inserting alarms

You can insert alarms into a configured Layer 2 CPRI signal.

To insert alarms

Step1 Verify the laser is active (Laser button is yellow).

Step2 Select an alarm type (**R-LOS, R-LOF, RAI, SDI**).

Step3 Press the **Alarm Insert** button.

The module inserts an alarm and the button turns yellow.

Test results associated with the alarm or defect appear in the Status result category.

Layer 2 OBSAI testing

If the instrument is optioned to do so, the Port Type, Enable LOS, Force Tx Idle and define the RP3 address and Type parameters can be specified in Layer 2 OBSAI applications.



NOTE:

OBSAI Layer 2 testing is not applicable to MSAMv1 or T-BERD/ MTS 8000v1 DMC.

OBSAI Layer 2 testing at 6144M rate is not available on T-BERD 5800.

To configure Layer 2 OBSAI testing

Step1 Using the Test Menu, select a OBSAI Layer 2 BERT Terminate application.

Protocol	Frequency	Applications
OBSAI	768.0M	Layer 2 BERT Terminate
	1536.0M	Layer 2 BERTTerminate
	3072.0M	Layer 2 BERTTerminate
	6144.0M	Layer 2 BERTTerminate

Step2 Select the **Setup** soft key, and then the OBSAI tab.

a In the Tx box, specify the **Port Type**, **LOS Enable**, **Force Tx Idle, Scrambler Seed**, **RP3 Address**, and **RP3 Type**.

b In the Rx box, specify the **RP3 Address** and **RP3 Type**.

c If scrambling is desired, check the Enable Seeds Exchange Box (6144M OBSAI only).

d If FCB message generation/detection is desired check Enable FCB message box.

Step3 Select the **Pattern** tab.

a Select a Pattern Mode.

b Select the desired pattern from the list of available patterns.

Step4 If service disruption detection is desired, select the **Service Disruption** tab and click the Enable checkbox. Define the parameters to be detected from the available selections.

Step5 If a timed or delayed start test is required, select the **Timed Test** tab and specify the desired start times and duration.

Step6 Select the **Results** soft key to return to the Main screen.

Step7 Select the Laser Tab at the bottom of the screen and click the **Laser On** button.

Step8 Select the CPRI result group and then choose a category to view:

- Error Stats
- Counts
- L1 Inband Protocol

You are testing CPRI layer 2.

Inserting errors

Action buttons on the Main screen allow you to insert errors into the CPRI/OBSAI signal. If you turn on a particular error insertion rate, the error insertion continues even after you restart a test or change the test configuration.

To insert errors

Step1 If you are inserting errors, select one of the following error types:

- Code
- K30.7
- BIT/TSE
- Running Disparity (CPRI L2 only)

Step2 Do the following:

- Specify the Insertion Style (**Single**, or **Rate**).
- If you specified Rate, select a rate.

Step3 Press the **Error Insert** button.

Error or pause frame insertion starts. If you are inserting errors at a particular rate, the associated button turns yellow. To stop insertion, press the corresponding button again. Error insertion stops, and the associated button turns gray.

Monitoring CPRI or OBSAI layer 1

If your instrument is optioned to do so, you can monitor CPRI or OBSAI links.

To monitor CPRI or OBSAI

Step1 Using the Test Menu, select a CPRI or OBSAI Monitor/Thru application.

Protocol	Frequency	Mon/Thru Applications
CPRI Layer 1	614.4M	P1 Mon/Thru P2 Mon/Thru
	1228.8M	P1 Mon/Thru P2 Mon/Thru
	2457.6M	P1 Mon/Thru P2 Mon/Thru
	3072.0M	P1 Mon/Thru P2 Mon/Thru
	4915.2M	P1 Mon/Thru P2 Mon/Thru
	6144.0M	P1 Mon/Thru P2 Mon/Thru
	9830.4M	P1 Mon/Thru P2 Mon/Thru

Protocol	Frequency	Mon/Thru Applications
CPRI Layer2	614.4M	Mon/Thru
	1228.8M	Mon/Thru
	2457.6M	Mon/Thru
	3072.0M	Mon/Thru
	4915.2M	Mon/Thru
	6144.0M	Mon/Thru
OBSAI Layer 1	768M[a]	P1 Mon/Thru P2 Mon/Thru
	1536M[a]	P1 Mon/Thru P2 Mon/Thru
	3072.0M[a]	P1 Mon/Thru P2 Mon/Thru
	6144.0M	P1 Mon/Thru P2 Mon/Thru
OBSAI Layer 2	768M	Mon/Thru
	1536M[a]	Mon/Thru
	3072.0M[a]	Mon/Thru
	6144.0M	Mon/Thru

a. Available on MSAMv1

Step2 To specify the BER pattern select the **Setup** soft key, and then the **Pattern** tab.

– *For Layer 1 CPRI/OBSAI* -Select the **Payload Analysis** checkbox if it is desired to check for BERT pattern errors.

This will cause pattern sync, bit errors etc. to be reported in the results.

– *For Layer 2 CPRI/OBSAI* - Select the **Pattern** tab.

Select the **Pattern Mode** desired.

Select the desired **Pattern** from the drop-down list.

Step3 *For Layer 2 OBSAI* - To specify the OBSAI Rx parameters, select the **OBSAI** tab.

– Select the **RP3 address** of the OBSAI receiver.

– Select the **RP3 type** from the drop-down list.

Step4 *For Layer 2 CPRI/OBSAI* -If service disruption detection is desired, select the **Service Disruption** tab.

– Click the Enable checkbox.

– Define the Separation Time and Threshold Time parameters by entering the desired values.

– Click the Event triggers tab.

– Click the events on the tabs for which service disruption notifications are desired.

Step5 If a timed or delayed monitoring is required, select the **Timed Test** tab and specify the desired start times and duration.

Step6 Press **Results** to return to the Main screen.

Step7 Connect the module to the circuit. If necessary, select either **SFP1** or **SFP2.**

Step8 Select the **Laser** button.

Step9 Verify that the green Signal LED is illuminated.

Step10 Press the **Restart** soft key.

You are monitoring CPRI or OBSAI.

4

Ethernet and IP Testing

This chapter provides information on testing Ethernet and IP services using the MSAM. Topics discussed in this chapter include the following:

– “About Ethernet and IP testing” on page 22
– “Cable Diagnostics” on page 32
– “Adjusting the frequency of transmitted optical signals” on page 34
– “Enabling automatic traffic transmission” on page 35
– “Discovering another JDSU test instrument using J-Connect” on page 36
– “Discovering network devices” on page 40
– “Programming JMEPs” on page 41
– “Protocol Analysis” on page 42
– “Layer 1 BER testing” on page 43
– “Layer 2 testing” on page 46
– “Layer 3 testing” on page 78
– “Capturing packets for analysis” on page 93
– “Loop back testing” on page 105
– “Inserting errors or pause frames” on page 105
– “Inserting alarms or defects” on page 106
– “Measuring round trip delay or packet jitter” on page 106
– “Measuring one way delay” on page 107
– “Measuring service disruption time” on page 118
– “OAM service and link layer testing” on page 119
– “MAC-in-MAC testing” on page 125
– “Synchronous Ethernet testing” on page 132
– “Transmitting and analyzing PTP/1588 traffic” on page 133
– “Discovering traffic using J-Profiler” on page 136

About Ethernet and IP testing

If your instrument is configured and optioned to do so, you can use it to provision Ethernet and IP service, verify end-to-end connectivity, and analyze link performance by simulating different traffic conditions. Figure 5 illustrates the Main screen when running an Ethernet application.

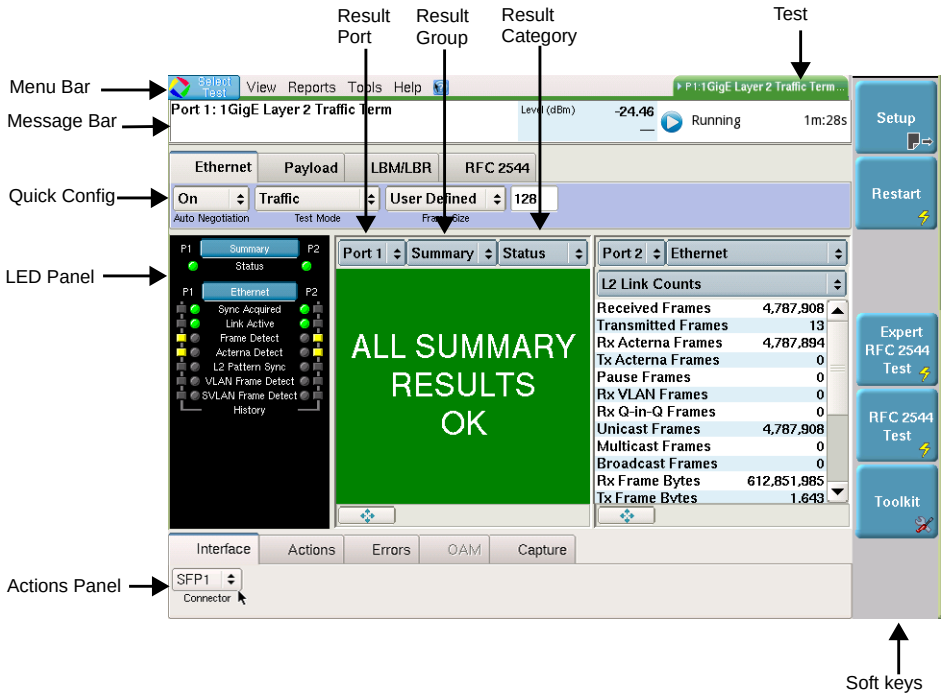


Figure 5 MSAM Main screen (Ethernet Terminate Application)

Features and capabilities

Features and capabilities include the following when testing Ethernet or IP service:

- 10/100/1000, 1 Gigabit Ethernet, 10 Gigabit LAN, 10 Gigabit WAN, 40Gigabit Ethernet and 100Gigabit Ethernet testing—Testing on each of these circuits is supported.
- JDSU Discovery—You can automatically detect other JDSU test equipment on the network, and determine their services and capabilities. For details, see “Discovering another JDSU test instrument using J-Connect” on page 36.
- Cable diagnostics—You can use the Dual Module Carrier, Transport Module, and MSAM to examine the state of the cables used to transmit 10/100/1000 electrical signals before you begin testing. For details, see “Cable Diagnostics” on page 32.
- Ping test during Setup—After entering the destination address (during application Setup or in the Quick Config bar in the Main Menu), the validity of the address entered can be checked in layer 3+ applications. The ping will be sent using the currently defined frame encapsulation and will be able to respond despite mismatched frames. Ping buttons will appear next to the Destination IP in the Quick Config bar on the main screen and on the IP/Source Destination Address page during Setup.
- Automatic traffic transmission—You can optionally set up optical Ethernet, IP, TCP/UDP, and Fibre Channel Traffic, Multiple Streams, and Triple Play applications to generate and transmit traffic automatically whenever you turn the laser on.

- Dual port testing—You can run a dual port test in terminate or through mode from a 10/100/1000 or 1GigE interface, and observe test results for each port simultaneously on the Main screen. Dual port testing requires two SFP or XFP PIMs (MSAM, CSAM, or 40/100G Transport Module).
- BER testing—You can verify circuit performance by sending BERT patterns over switched (layer 2) and unswitched (layer 1) networks. You can also configure ATP payloads carrying a BERT pattern.
- Multiple source MAC addresses—When transmitting a single stream of Layer 2 traffic, you can simulate traffic from multiple sources by assigning a range of MAC addresses to be carried in the frames transmitted in the stream.
- Layer 2 transparency testing—You can transmit and analyze layer 2 traffic with *CDP, VTP, STP, and R/STP headers* to verify that a circuit can support a variety of control protocols irrespective of the transport method. For details, see “Using J-Proof to verify layer 2 transparency” on page 74.
- Automated VLAN testing—An automated VLAN test is available that tests a range of VLANs by transmitting and looping back frames for each VLAN in the range for a user-specified test period, and then comparing the number of frames transmitted to the number received. For details, see “Automated VLAN tests” on page 317.
- Layer 3 testing—You can perform end to end tests to verify throughput. You can also:
  - Transmit packets and determine if any are lost when looped back to your module.
  - Filter traffic using layer 3 criteria.
  - Measure round trip delay. 10M/100M/1GbE/10GbE, 40G/100G data rates can utilize ATP version 3 for highly accurate delay measurements.
  - Send ping requests and respond to ping requests from another Ethernet device to verify connectivity.
  - Record and observe the route of traffic through the network using the Traceroute application.
  - Insert IP checksum errors into the traffic stream.
  - Insert Acterna payload errors into the traffic stream.
- J-Profiler traffic explorer—You can use the J-Profiler application to automatically discover and monitor up to 128 streams of traffic that satisfy your profile criteria on 10/100/1000 electrical, 100M optical, and 1GigE optical circuits. For details, see “Discovering traffic using J-Profiler” on page 136.
- PPPoE support—If your instrument is configured and optioned to do so, you can configure your unit to emulate a PPPoE client or server, login to a PPP peer to establish a PPPoE session, and then transmit IPv4 packets over an Ethernet circuit for analysis. For details, see “Specifying L3 interface settings” on page 79 and “Configuring MPLS traffic” on page 80.
- IPv6 support—If you purchased the IPv6 Traffic option, you can transmit and analyze IPv6 traffic using the terminate and monitor/thru applications. When configuring your test, you can specify the required addresses manually, or you can use stateless or stateful auto-configuration to assign addresses for you.
- Packet capture and analysis—If your instrument is configured and optioned to do so, you can use it to capture transmitted and received data, save it on the instrument or to a USB key, and then either send the data to another technician for analysis, or analyze it yourself using the Wireshark® protocol analyzer (provided on the instrument). For details, see “Capturing packets for analysis” on page 93. In addition, if capturing VoIP packets, the data can by analyzed with the PVA-1000 utility from JDSU.
  NOTE: PVA-1000 is used for VoIP analysis only.
- MPLS and VPLS testing—If you purchase the MPLS/VPLS test option, you can configure your unit to generate, transmit, and analyze MPLS and VPLS encapsulated frames when testing

and qualifying core and metro networks. For details, see "Configuring MPLS over Ethernet tests" on page 30 and "Configuring Ethernet VPLS tests" on page 29.

– Q-in-Q testing—You can configure, transmit, and analyze traffic carrying SVLAN and CVLAN tags per IEEE 802.1ad to verify that your network can support and prioritize traffic for multiple customers without conflicts. You can also specify a user-defined TPID for the service provider when transmitting and filtering Q-in-Q encapsulated traffic. For details, see "Configuring Q-in-Q traffic" on page 55.

– MiM testing—If you purchase the MiM testing option, you can transmit and analyze MAC-in-MAC Ethernet traffic over a PBB (Provider Backbone Bridged) network to verify end-to-end connectivity, and analyze link performance. For details, see "MAC-in-MAC testing" on page 125.

– Stacked VLAN—If your instrument is configured and optioned to do so, you can configure, transmit, and analyze L2 traffic carrying SVLAN and CVLAN tags per IEEE 802.1ad to verify that your network can support and prioritize traffic for multiple customers without conflicts. You can also specify a user-defined TPID for the service provider when transmitting and filtering stacked VLAN encapsulated traffic. For details, see "Configuring stacked VLAN traffic" on page 55.

– Trigger support. The instrument supports packet capture based on a triggering event. For details, see "Capturing packets based on a trigger" on page 97.

– Filters enhanced to include byte pattern filter. The instrument supports filtering on a 16-byte pattern. For details, see "Filtering traffic using byte pattern criteria" on page 62

– Link and service layer OAM testing—OAM messages are supported, enabling you to identify trunk problems so you can initiate a switch to a protection path. When testing Ethernet First Mile OAM communications, you can loop back an adjacent node or Ethernet demarcation device (EDD), and then exchange messages with the node or device to verify that auto-discovery and error notification are functioning properly. For details, see "OAM service and link layer testing" on page 119.

– Packet jitter testing—You can verify the integrity of triple play services such as Video and VoIP by qualifying the packet jitter characteristics of Ethernet circuits. For details, see "Measuring round trip delay or packet jitter" on page 106.

– OTN testing—If you purchased an instrument configured for OTN testing, you can generate and transmit 10 Gigabit LAN Ethernet payloads at OTU-2 line rates (11.05G and 11.1G) or 1 Gigabit Ethernet payloads utilizing ODU0 multiplexing carried in an OTU-2 or OTU-1 wrapper over an OTN circuit. If you purchased a 40G/100G High Speed Transport Module configured for OTN testing, you can generate and transmit Bulk BERT payloads at OTU-3 line rates (43.02G) or OTU4 line rates (111.8G) and 100 Gigabit Ethernet payloads utilizing ODU4 multiplexing carried in an OTU-4 wrapper over an OTN circuit. For details, see the *PDH, SONET, SDH, NextGen, and OTN Testing Manual* that shipped with your instrument or upgrade.

– NextGen GFP testing—If your instrument is configured and optioned to do so, you can use it to transmit and analyze generic framing procedure (GFP) traffic carrying Ethernet frames over a legacy SONET or SDH circuit, and then run layer 2 and layer 3 Ethernet tests to verify that network performance conforms to all applicable ITU-T and IEEE standards. For details, see the *PDH, SONET, SDH, NextGen, and OTN Testing Manual* that shipped with your instrument or upgrade.

– Test Access Management (TAM)—If your instrument is configured and optioned to do so, you can now use it to remotely log into and provision network elements such as switches and routers from a Mobility Switching Center (MSC). You can also use your instrument to emulate a router on the network end of the Ethernet Transport Service (ETS), run an RFC 2554 script to put a Network Interface Device (NID) in loop back mode, transmit traffic, then analyze looped back traffic to determine link characteristics such as throughput and latency. For details, see "Testing using TAM automation" on page 332 of Chapter 12 "Automated Testing".

– One way delay measurements—If your instrument is configured and optioned to do so, you can measure delay in one direction on a circuit. For details, see “Measuring one way delay” on page 107.

– Sync-E timing- If configured and optioned to do so, the instrument can provide physical layer timing transport required to guarantee frequency distribution to the extent necessary for encapsulated signals to meet network performance requirements. Transmit capability is available on 100M/1GE/10GE Optical all layer applications except J-Profiler, IPTV, VoIP, Wirespeed, L1 BERT and thru modes. Detection is available on the same interfaces as well as 10/100/1000 Electrical Ethernet applications on MSAMv2, only if a SyncE PIM is installed.

Understanding the graphical user interface

When you configure your module for testing, graphical displays of Ethernet frames and IP packets are provided on the setup tabs for the application you selected. You can specify frame or packet characteristics for transmitted and filtered traffic by selecting the corresponding field on the graphic, and then entering the value for transmitted or filtered traffic. Colored fields can be edited; fields in gray can not be modified.

Frame settings

Figure 6 illustrates the frame settings for a layer 2 traffic test, with the Data field selected.

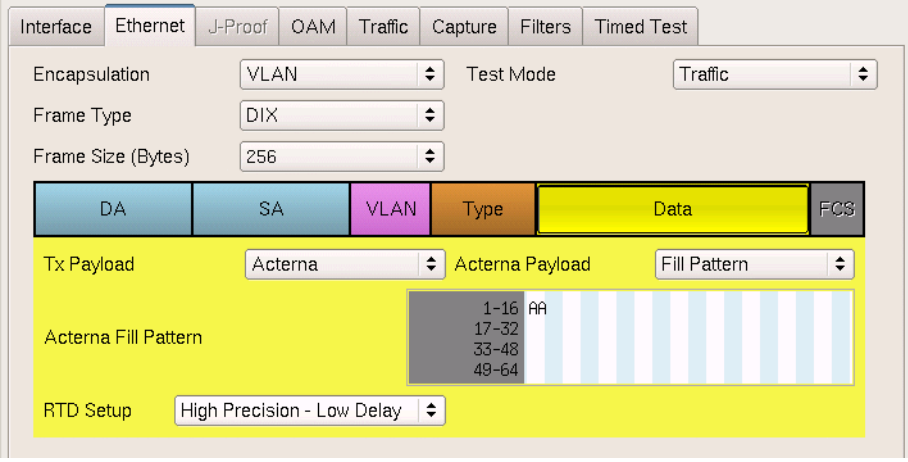


Figure 6 Frame Settings

For details on each of the settings, see “Specifying Ethernet frame settings” on page 49 and “Specifying Ethernet filter settings” on page 56.

Packet settings

Figure 7 illustrates the IP packet settings for a layer 3 traffic test.

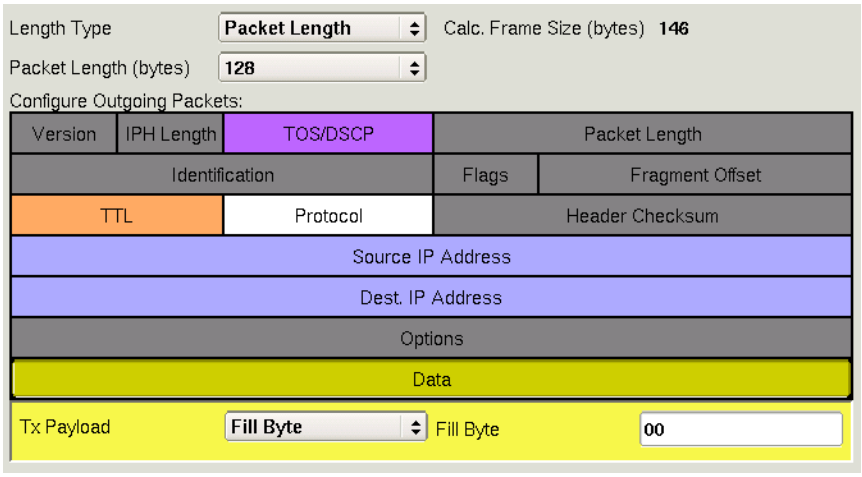


Figure 7 IP Packet Settings

For details on each of the settings, see "Specifying transmitted IPv4 packet settings" on page 83 and"Specifying IPv4 filter settings" on page 85

Ethernet and IP test applications

This release supports the layer 2 and layer 3 applications listed in Table 2.

- MiM applications are listed in Table 3 on page 27.
- Layer 4 TCP/UDP applications are listed in Table 12 on page 149 of Chapter 6 "TCP/UDP Testing".
- Multiple Streams applications are listed in Table 13 on page 168 of Chapter 7 "Triple Play and Multiple Streams Testing"
- Triple Play applications are listed in Table 15 on page 181 of Chapter 7 "Triple Play and Multiple Streams Testing".
- Loop back applications are listed in Table 16 on page 194 of Chapter 8 "Loop back Testing".

Table 2 Ethernet and IP applications

Application	Test Mode	10/100/1000	100M Optical	1 GigE Optical	10 GigE LAN	10 GigE WAN	40Gig & 100Gig Optical
Layer 1 PCS	Terminate	N/A	N/A	N/A	N/A	N/A	√
Layer 1 BERT	Terminate Monitor/Through	N/A	N/A	√	√	√	N/A
Layer 2 Patterns	Terminate	N/A	N/A	√	√	N/A	N/A
Layer 2 Traffic	Terminate Monitor Monitor/Through	√ √	√ √	√ √	√ √	√ √	√ √
Layer 3 Ping[a]	Terminate	√	√	√	√	√	√

Table 2 Ethernet and IP applications (Continued)

Application	Test Mode	10/100/1000	100M Optical	1 GigE Optical	10 GigE LAN	10 GigE WAN	40Gig & 100Gig Optical
Layer 3 Traceroute[a]	Terminate	√	√	√	√	√	√
Layer 3 Traffic[a]	Terminate Monitor Monitor/Thru	√ √	√ √	√ √	√ √	√ √	√ √

a. IPv4 and IPv6 applications are available. IPv4 and IPv6 applications are also available when running layer 3 and layer 4 multiple streams terminate applications.

MiM test applications

If your instrument is optioned to do so, this release supports the MiM (MAC-in-MAC) applications listed in Table 3.

Table 3 MiM applications

Interface	Application	Test Mode
10/100/1000	MiM Traffic	Terminate Monitor
100M Optical	MiM Traffic	Terminate Monitor
1GigE Optical	MiM Traffic	Terminate Monitor
10GigE LAN	MiM Traffic	Terminate Monitor/Through

MPLS-TP test applications

If your instrument is optioned to do so, this release supports the MPLS-TP applications listed in Table 4.

Table 4 MPLS-TP applications

Interface	Application	Test Mode
10/100/1000	Layer 2 MPLS-TP Traffic	Terminate
100M Optical	Layer 2 MPLS-TP Traffic	Terminate
1GigE Optical	Layer 2 MPLS-TP Traffic	Terminate
10GigE LAN	Layer 2 MPLS-TP Traffic	Terminate

PTP/1588 test applications

If your instrument is optioned to do so, this release supports the PTP/1588 applications listed in Table 5.

Table 5 PTP/1588 applications

Interface	Application	Test Mode
10/100/1000	Layer 2 PTP/1588 Layer 4 PTP/1588	Terminate
100M Optical	Layer 2 PTP/1588 Layer 4 PTP/1588	Terminate
1GigE Optical	Layer 2 PTP/1588 Layer 4 PTP/1588	Terminate

Configuring applications in Dual Through mode

When configuring applications in Dual Through modes, you must specify test and traffic settings for each port.

If you are currently running tests using both ports, you must remove one test before launching a Dual Through mode application.

To configure an application using two ports

Step1 Launch an application in Dual Through mode.

Step2 Use the Port Selection soft key to select a port.

Step3 Configure the test running on the port. The settings you specify will apply only to the *currently selected por*t.

Step4 Use the Port Selection soft key to select the second port, then configure the second test.

When running applications in Dual Through mode, the user interface behaves as follows:

Quick Config settings—The Quick Config tab located under the Message Bar, provides key settings required to configure the currently selected Port. *Changing a setting that prompts an automatic restart on one port also restarts the test or script running on the other port*.

LEDs—LEDs are provided for Port 1 and Port 2 (see Figure 5 on page 22).

Action Panel—The Action buttons affect the *currently selected port.*

Restart Soft key—The Restart soft key affects *both ports*; therefore, script results will be reset (and inaccurate) if you press Restart while running a script on one port. If you are running a script, wait for the script to complete before pressing Restart.



DUAL PORT TEST RESULTS:

Although you can only perform actions on the currently selected port, you can easily observe test results for both ports without toggling back and forth. To do so, set the result port in one pane to Port 1, and the result port in a second pane to Port 2.

Configuring 10 Gigabit Ethernet WAN tests

– When you use the instrument to test 10 Gigabit WAN interfaces, you can specify settings that characterize the SONET or SDH network in addition to the settings used to characterize the Ethernet data. Essentially, the setup tabs are a combination of those used to specify SONET or SDH settings, and those used for the Ethernet applications discussed in this chapter. When configuring the module to test a WAN interface, refer to the *PDH, SONET, SDH, NextGen, and OTN Testing Manual* that shipped with your instrument or upgrade for details on each of the SONET/SDH setup tabs.

NOTE:
When configuring the module for WAN testing, default SONET/SDH overhead values are per IEEE 802.3ae.

Configuring Ethernet VPLS tests

The instrument allows you to configure and transmit layer 2 VPLS traffic (see Figure 8) by specifying tunnel and virtual circuit label settings.

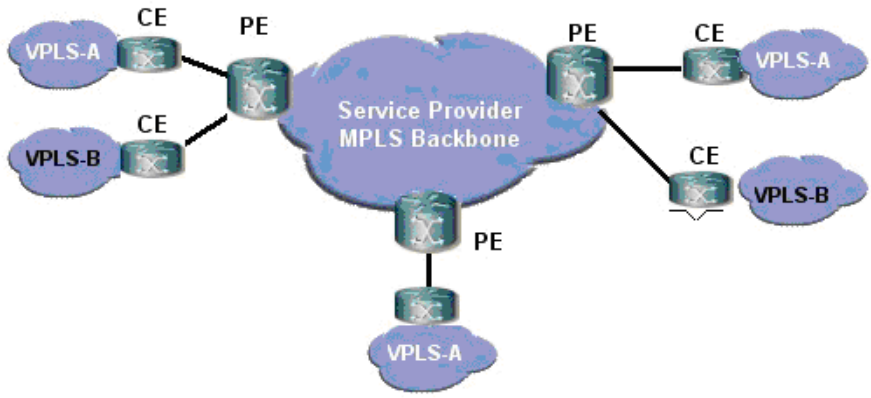


Figure 8 VPLS network

Figure 9 illustrates generic tunnel and virtual circuit (VC) labels, which together comprise a VPLS header. Shaded fields are user-configurable.

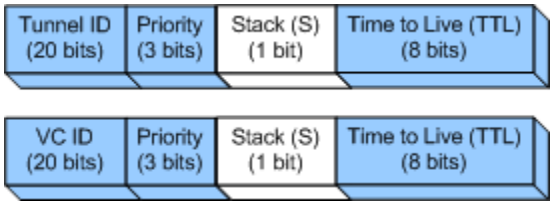


Figure 9 Generic tunnel and VC labels

When configuring traffic for VPLS testing, be certain to specify labels that have already been instantiated by routers on the network. For details on specifying VPLS settings for transmitted traffic, see “Specifying Ethernet frame settings” on page 49. For details on filtering received VPLS traffic, see “Specifying Ethernet filter settings” on page 56.

VPLS tunnels

In a VPLS network, customer sites are connected to the service provider network (see Figure 8 on page 29) via PE routers. Each PE router in the network is connected together using tunnels, and can be connected to any other PE router residing on the network.

Virtual channels

Each tunnel is comprised of multiple channels which are used to carry different types of service between the PE routers.

VPLS test applications

Key VPLS applications include:

End-to-end testing of VPLS networks—For this application, you configure your unit to transmit layer 2 traffic *without a VPLS header* to a second unit on the far end of the circuit. The ingress provider edge (PE) router then adds the VPLS header and sends the encapsulated traffic through the network. The egress PE router removes the tunnel label. If the VPLS header also carries a VC label, the router forwards the traffic to the appropriate interface. Finally, the far end unit analyzes the received layer 2 traffic.

PE router emulation—For this application, you configure a unit on the near-end to emulate an *ingress PE router* transmitting VPLS encapsulated traffic to a second unit on the far end. Transmitted traffic is then routed through the VPLS network using the tunnel label you specified. The egress PE router removes the tunnel label. If the VPLS header also carries a VC label, the router forwards the traffic to the appropriate interface.

Traffic analysis: monitor mode— For this application, you configure a near-end unit to transmit layer 2 Ethernet traffic to an ingress PE router. The PE router then adds the VPLS header, and sends it through the network. Using a second unit, you connect to the circuit from a port provided by a router, and then monitor and analyze the VPLS encapsulated traffic.

Traffic analysis: through mode— For this application, you configure a near-end unit to transmit layer 2 Ethernet traffic to an ingress PE router. The PE router then adds the VPLS header, and sends it through the network. Using a second unit, you connect to the circuit at a point between the two routers, monitor and analyze the received VPLS encapsulated traffic, and then pass the traffic through the unit to transmit it to the next router on the network.

Configuring MPLS over Ethernet tests

The instrument allows you to transmit layer 3 IP traffic over a MPLS network by specifying MPLS label settings. Figure 10 illustrates a generic MPLS header. Shaded fields are user-configurable.



Figure 10 Generic MPLS header

When configuring traffic for MPLS testing, be certain to specify labels that have already been instantiated by routers on the network. For details on specifying MPLS settings for transmitted traffic, see "Specifying Ethernet frame settings" on page 49. For details on filtering received MPLS traffic, see "Specifying Ethernet filter settings" on page 56.

Key MPLS test applications include:

End-to-end testing of MPLS networks—For this application, you configure your unit to transmit layer 3 traffic *without MPLS labels* to a second unit on the far end of the circuit. The ingress provider edge (PE) router then adds the MPLS header and sends the encapsulated packet through the network. The egress PE router removes the MPLS header, and then forwards the data to a second unit on the far end. The far end unit then analyzes the layer 3 traffic.

PE router to CE router emulation—For this application, you configure a unit on the near-end to emulate an *ingress PE router* transmitting MPLS encapsulated traffic to a second unit on the far end. The far end unit is configured to emulate a *customer edge (CE) router*. If the network uses routers which do not use ARP, you may also need to specify the MAC address of the PE router that your near-end unit is connected to. Transmitted traffic is then routed through the MPLS network using the MPLS header settings you specified. The egress PE router removes the MPLS header, and then forwards the layer 3 IP traffic to the far end unit (which is emulating a CE router) for layer 3 analysis.

PE router to PE router emulation—For this application, you configure a unit on the near-end to emulate an *ingress PE router* transmitting MPLS encapsulated traffic to a second unit on the far end. The far end unit is configured to emulate an *egress PE router*. If the network uses routers which do not use ARP, you may also need to specify the MAC address of the PE router that your near-end unit is connected to. Transmitted traffic is then routed through the MPLS network using the MPLS header settings you specified. The far end unit emulating the egress PE router removes the MPLS header, and analyzes the layer 3 IP traffic.

Core router testing—For this application, you configure a unit on the near-end to emulate an i*ngress PE router*, which then transmits MPLS encapsulated traffic to a *core router* on the MPLS network. Using the label you specified for the traffic originated by the near-end unit, the core router forwards the traffic to a second far end unit, which is configured to emulate another router in the core of the network. The far end unit then analyzes received traffic (based on the MPLS filter criteria you specified) to determine the characteristics of the *intermediary core router*.

Packet analysis: monitor mode— For this application, you configure a near-end unit to transmit layer 3 IP traffic to a ingress PE router. The PE router then adds the MPLS header, and sends it through the network. Using a second unit, you connect to the circuit from a port provided by a core router, and then monitor and analyze the MPLS encapsulated traffic.

Packet analysis: through mode— For this application, configure a near-end unit to transmit layer 3 traffic to a ingress PE router. The PE router then adds the MPLS header, and sends it through the network. Using a second unit, you connect to the circuit between two routers, monitor and analyze the received MPLS encapsulated traffic, and then pass the traffic through the unit to transmit it to the next router on the network.

Configuring IPv4 and IPv6 tests

If you purchased the IPv6 option, applications are provided that allow you to transmit and analyze either IPv4 or IPv6 traffic. Table 6 lists the key differences between the applications:

Table 6 IPv4 and IPv6 applications

Feature	IPv4	IPv6
Source IP Configuration	– In IPoE mode, uses DHCP or manual configuration. – In PPPoE mode, uses the client-server PPPoE login process. For details, see "Configuring MPLS traffic" on page 80.	Uses one of the following: – Stateful Auto-configuration (also known as DHCPV6) – Stateless Auto-configuration – Manual configuration
Source IP Address	A single IP address is assigned to the interface transmitting IP traffic.	Two IP addresses are assigned: – Link-local address. this source address is assigned locally, and must always go through duplicate address detection (DAD). – Global address. This second source address is not used locally; it is used to transmit traffic beyond the router.
Automatic MAC Address Resolution	Uses ARP	Uses Neighbor Solicitation
Traffic prioritization	Uses one of the following: – *Layer 2* VLAN or Q-in-Q encapsulation. – *Layer 3* MPLS encapsulation which uses labels and tunnel priorities.	Uses the following: – VLAN or Q-in-Q encapsulation. – Flow labels. The instrument allows you to configure traffic with flow labels simply to determine whether routers on the circuit support the labels. – MPLS encapsulation is not supported.
IP Header Checksums	Checksum error insertion supported.	Does not use checksums.
Error Messages	ICMPv4 messages appear.	ICMPv6 messages appear.

Cable Diagnostics

Before testing 10/100/1000 electrical Ethernet, IP (IPoE), or TCP/UDP circuits, you can use the instrument to examine the state of the cables used to transmit electrical signals. Typically this involves out-of-service testing to determine the link status, the pair status of each MDI or MDI-X pair, the pair assignments for 1000M links, the polarity for each MDI pair, and the pair skew. You can also use the instrument to verify whether or not Power over Ethernet (PoE) service is available on the link (per IEEE 802.3af). Finally, if the link is inactive, you can use the instrument to determine the nature of the fault.

Cable diagnostics should not be run in PPPoE Data Mode when running layer 3 test applications.

Running cable diagnostics

Running cable diagnostics involves connecting to the link, launching the Cable Diagnostics tool, and then observing the measurements provided on the Cable Diagnostics screen.

To run cable diagnostics

Step1 If you haven't already done so, turn ON the Transport Module, and launch a 10/100/1000 electrical Ethernet application, and verify that Auto-negotiation is turned ON.

Step2 Select the **Toolkit** soft key, and then select the **Cable Diagnostics** tool.

The Cable Diagnostics screen appears.

Step3 Connect the Transport Module to the link.

Step4 Verify that traffic is not being transmitted. The Start Traffic action button should be *gray*.

Step5 To start the diagnostics, select **Analyze Cable**.

Step6 Observe the cable results and measurements.

Cable diagnostics are complete.

Viewing cable measurements

Cable measurements appear automatically on the Cable Diagnostics screen (see Figure 11).

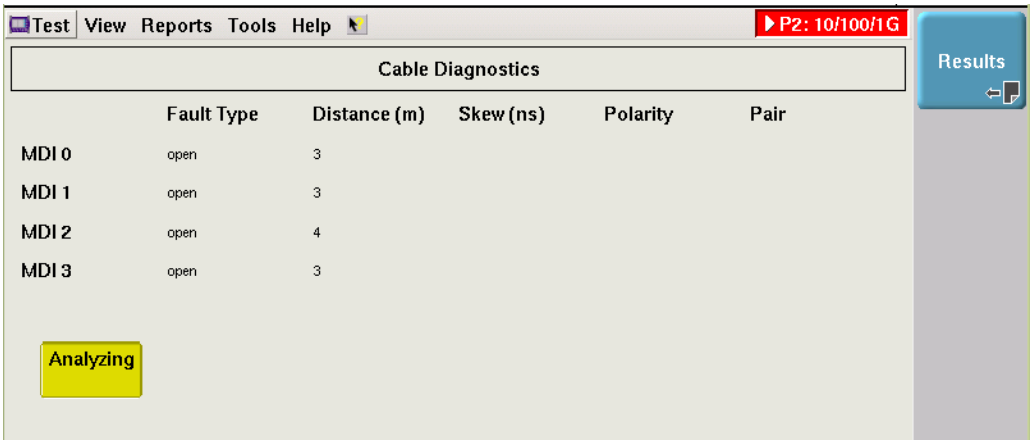


Figure 11 Cable Diagnostics screen

For detailed descriptions of each of the measurements, see "Cable Diagnostic results" on page 351.

Skew Injection

For all 40G and 100G OTL applications, you can specify bit-level static skew injection at the lane level and specify the threshold of excess static skew. On the CSAM, skew injection is available on 40G applications.

To inject skew

Step1 Using the Test Menu, select the interface and test application for the signal, rate, and payload being tested. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key.

Step3 On the interface tab, select the Bit Skew Injection subtab. Specify the amount of skew (in bits) for each Physical Lane to be tested (0-64000). When the number of bits is entered for a lane, the Injected Skew (in ns) will be calculated for the current configuration. To return all lane skew settings to 0, press the **Default** button.

Step4 Select the Signal subtab. In the Skew Alarm frame, specify the threshold (in ns) for which the unit should report a Static Skew alarm.

Step5 Select the **Results** soft key to return to the Main screen, or select another tab to specify additional test settings.

Skew injection is set.

Adjusting the frequency of transmitted optical signals

If your unit is configured and optioned to do so, you can adjust the frequency of transmitted optical signals in 1 PPM increments. Before adjusting the frequency, consider the following:

– If you are transmitting traffic to another unit placed in LLB mode, if you increase the frequency you may overrun the LLB unit. As a result, the transmitting unit will report lost frames and out of sequence frames in the traffic received from the LLB unit.
– Increasing the frequency may also overrun certain network devices on the circuit you are testing.

To adjust the frequency

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Connect the module to the circuit.

Step3 Select the **Laser** button.

Step4 Select the Laser action bar, and then do one of the following:

– To increase the frequency by 1 PPM, press Freq Offset +1.
– To decrease the frequency by 1 PPM, press Freq Offset -1.

You increase or decrease the frequency up to 100 PPM.

Step5 On the transmitting unit, observe the values for the following results in the Interface result group, Signal category:

– `Tx Freq Max Deviation (ppm)`
– `Tx Frequency Deviation (ppm)`

Step6 On the receiving unit, verify that the values for the following results match the transmitted frequency values.

– `Rx Freq Max Deviation (ppm)`
– `Rx Frequency Deviation (ppm)`

The frequency was adjusted.

Enabling automatic traffic transmission

You can optionally set up Ethernet LAN, IP, TCP/UDP, and Fibre Channel test applications to generate and transmit traffic automatically whenever you turn the laser on (for optical applications).

Prerequisites for traffic transmission

If you enable automatic traffic generated, traffic is transmitted after the following occurs:

– You turn the laser ON (using the Laser ON action button).
– A signal is acquired.
– Synchronization is acquired.
– A link is established.
– If you are running a layer 3 (IP) application and ARP is enabled, ARP must be successful. If ARP is not enabled, the destination IP address must be available.
– If you are running a Fibre Channel application, the login process must be complete.

As always, you can turn traffic off at any time using the **Stop Traffic** action button.

Issues to consider

Consider the following issues and behavior before enabling automatic traffic generation:

– **This is not a global setting.** This setting does not affect all Ethernet LAN, IP, TCP/UDP, and Fibre Channel applications; you must enable automatic traffic generation for *each individual application*. After you enable the setting for a particular application, it will remain enabled until you disable it.
– **Changing setups while tests are running.** Your unit is designed to handle traffic transmission appropriately when you change key setups while a test is running. In some instances, if you change key setups while running a test, traffic stops temporarily (as a result of the changed setup), and then starts again. In other instances, changing a setup stops traffic entirely until you actively start it again.

  This is still the case when automatic traffic generation is enabled. If you change a setup that causes the unit to stop transmitting traffic entirely, you must actively start it again by pressing the **Start Traffic** action button.
– **Loop back testing.** Ensure that your unit is not placed in loop back mode by verifying that the LLB action button is gray. If you intend to issue a command to loop up another unit, make certain automatic traffic generation is not enabled on the far end unit. If it is not disabled, the far end unit will not respond to the loop up command.

Issues specific to certain applications are explained in the associated procedures provided in this chapter.

Enabling the feature

To enable automatic traffic generation

Step1 Using the Test menu, launch the test application for the optical interface you are about to test.

Step2 Select the Setup soft key, and then do the following:

a Select the Interface tab.

b Select the Physical Layer sub-tab.

c Set *Auto-start traffic when laser turned on* to **Yes**.

Traffic will be transmitted after you turn the laser on and the criteria listed in "Prerequisites for traffic transmission" on page 35 is satisfied.

Discovering another JDSU test instrument using J-Connect

When testing using an MSAM, you can automatically detect other JDSU test instruments on the same subnet and determine their capabilities.You can then optionally configure key parameters for your test automatically based on a discovered instrument's settings.



NOTE:

The J-Connect feature is not available when using a 40G/100G High Speed Transport Module.

When your instrument discovers the other instruments on the subnet, it is simply providing a snapshot of the information available for the instruments at that current time. If someone changes an instrument's IP address, or disconnects an instrument from the circuit, this will not be reflected in the snapshot. To ensure that you have accurate data, you should refresh the display periodically. The instruments must be on the same VLAN ID and ether types.

The J-Connect feature is not available when testing using the Transport Module, or when running MAC-in-MAC, multiple stream, IPv6, IP Video, or Triple Play applications.

Discoverable instruments

Discoverable test instruments include:

– The T-BERD/MTS 8000, 6000A, and 5800
– The T-BERD/MTS 8000 Transport Module
– The T-BERD/MTS 6000A MSAM
– HSTs with Ethernet SIMs

Prerequisites

To be discoverable, JDSU test instruments must:

– Run a software version that supports the J-Connect feature.
– Be configured to be discoverable.
– Have a unique source IP address. JDSU test instruments of the same type (for example, MSAMs) ship from the factory with the same default source IP address. If you want to discover the instrument on the subnet, be certain to specify a different source IP address.

On the transmitter side, destination addresses and port numbers can be discovered. On the receiver side, source addresses and port numbers can be discovered. If you want to use a discovered instrument's MAC and IP addresses or port numbers to configure the settings on your instrument, verify the following:

– In the Ethernet menu, verify that the Destination Type is Unicast.

– In the Ethernet Filter, verify that the Source Type is Unicast.
– In the IP Filter, verify that the filter is enabled, and that the Source IP setting is checked.
– In the TCP/UDP Filter, verify that the filter is enabled, and that the service type for the source port is User Defined.
– Verify that you are not transmitting traffic.
– If you want to use the discovered MAC address as the destination address, turn ARP off if you are running a layer 3 or layer 4 application.

Discovering an instrument

To discover another JDSU test instrument

Step1 Before testing, ensure that instruments on the subnet are discoverable by doing the following for each:

a Launch a single-stream IPv4 terminate application (see "Step 1: Selecting a test application" on page 2).

b On the Main screen, above the result panes, select the J-Connect tab, and then verify that the **Make this unit discoverable** setting is selected.

c Verify that a different source IP address is assigned to each instrument. To observe the IP settings used for remote connections and the J-Connect feature, if you are running a layer 2 application, go to the Network Visibility sub-tab (on the Interface set up tab). If you are running a layer 3 or layer 4 application, the source IP address appears on the IP setup tab. This is also the IP address that a remote instrument must use to connect to the instrument when running the Asymmetric RFC 2544 test.

Step2 Connect your instrument to the circuit, and then do the following:

a Launch a single-stream layer 2, layer 3 (IPv4), layer 3 PING, or layer 4 terminate application.

b Verify that the Sync Acquired and Link Active LEDs are illuminated, indicating that an active link is established.

Step3 Verify that you are not running a timed test on any port.

Step4 If you haven't already done so, select the J-Connect tab on the Main screen, then select **Discover Units**.

A message appears asking you to wait while the instrument discovers devices.

If the instrument discovered other test instruments, their unit identifiers appear on the Discovered Devices screen.

If the instrument does not discover any other test instruments, a message appears stating that no devices were discovered, and instructing you to press **Refresh** to start the process again.



NOTE:

The J-Connect feature is also available when specifying destination MAC or IP addresses, or port numbers for transmitted traffic, or source MAC or IP addresses, or port numbers for filtered traffic.

About the Refresh key

The Refresh key appears whenever the Discovered Devices screen is displayed. Use the button to rediscover devices on the subnet (for example, if you suspect a discovered device is no longer connected to the circuit).

Sorting discovered instruments

By default, discovered instruments are listed by their unit identifiers. You can optionally sort them by serial number, application name, MAC, or IP address.

To sort discovered instruments

Step1 Discover the instruments.

Step2 On the Discovered Devices screen, select the **Display By ...** drop down list.

Step3 Select the sort key.

The instruments are sorted using the new key.

The application names that appear on the screen are abbreviated due to space constraints. Refer to Table 7 for the application name as it is typically used.

Table 7 Discovered application names

Discovered Name	Application Name
TermEth100ML2Loopback	100M Optical Eth Layer 2 Loopback Term
TermEth100ML2Traffic	100M Optical Eth Layer 2 Traffic Term
TermEth100ML3Loopback	100M Optical Eth Layer 3 Loopback
TermEth100ML3Ping	100M Optical Eth Layer 3 Ping Term
TermEth100ML3Traffic	100M Optical Eth Layer 3 Traffic Term
TermEth100ML4Loopback	100M Optical Eth Layer 4 Loopback
TermEth100ML4Traffic	100M Optical Eth Layer 4 Traffic Term
TermEth10GL2Loopback	10GigE LAN Layer 2 Loopback
TermEth10GL2Traffic	10GigE LAN Layer 2 Traffic Term
TermEth10GL3Loopback	10GigE LAN Layer 3 Loopback
TermEth10GL3Ping	10GigE LAN Layer 3 Ping Term
TermEth10GL3Traffic	10GigE LAN Layer 3 Traffic Term
TermEth10GL4Loopback	10GigE LAN Layer 4 Loopback
TermEth10GL4Traffic	10GigE LAN Layer 4 Traffic Term
TermEth10ML2Loopback	10/100/1000 Eth Layer 2 Loopback
TermEth10ML2Traffic	10/100/1000 Eth Layer 2 Traffic Term
TermEth10ML3Loopback	10/100/1000 Eth Layer 3 Loopback
TermEth10ML3Ping	10/100/1000 Eth Layer 3 Ping Term
TermEth10ML3Traffic	10/100/1000 Eth Layer 3 Traffic Term
TermEth10ML4Loopback	10/100/1000 Eth Layer 4 Loopback

Table 7 Discovered application names (Continued)

Discovered Name	Application Name
TermEth10ML4Traffic	10/100/1000 Eth Layer 4 Traffic Term
TermEth1GL2Loopback	1GigE Layer 2 Loopback
TermEth1GL2Patterns	1GigE Layer 2 Patterns Term
TermEth1GL2Traffic	1GigE Layer 2 Traffic Term
TermEth1GL3Loopback	1GigE Layer 3 Loopback
TermEth1GL3Ping	1GigE Layer 3 Ping Term
TermEth1GL3Traffic	1GigE Layer 3 Traffic Term
TermEth1GL4Loopback	1GigE Layer 4 Loopback
TermEth1GL4Traffic	1GigE Layer 4 Traffic Term
TermOc192Sts192cEthL2Loopback	10GigE WAN OC-192c Layer 2 Loopback
TermOc192Sts192cEthL2Traffic	10GigE WAN OC-192c Layer 2 Traffic Term
TermOc192Sts192cEthL3Loopback	10GigE WAN OC-192c Layer 3 Loopback
TermOc192Sts192cEthL3Ping	10GigE WAN OC-192c Layer 3 Ping Term
TermOc192Sts192cEthL3Traffic	10GigE WAN OC-192c Layer 3 Traffic Term
TermStm64Au464cVc464cEthL2Loopback	10GigE WAN STM-64 Layer 2 Loopback
TermStm64Au464cVc464cEthL2Traffic	10GigE WAN STM-64 Layer 2 Traffic Term
TermStm64Au464cVc464cEthL3Loopback	10GigE WAN STM-64 Layer 3 Loopback
TermStm64Au464cVc464cEthL3Ping	10GigE WAN STM-64 Layer 3 Ping Term
TermStm64Au464cVc464cEthL3Traffic	10GigE WAN STM-64 Layer 3 Traffic Term

Observing details for an instrument

After discovering the instruments, you can observe details for a particular instrument, and indicate whether or not you want to use the discovered instrument's MAC and IP address, and port number (if applicable) when you configure your instrument.

To observe details for a discovered instrument

Step1 Select the instrument on the Discovered Devices screen.

The Device Details screen appears to the right.

Step2 If you want to automatically apply the discovered instrument's MAC or IP address, or port number to your instrument's configuration, do the following:

a To use the discovered instrument's MAC or IP address, or port number as the destination MAC or IP address, or port number for your transmitted traffic, highlight the check box under Tx, and then select **Configure Checked Item(s)**.

b To filter received traffic using the discovered instrument's source MAC or IP address, or port number, highlight the check box under Rx, and then select **Configure Checked Item(s**).

Step3 Press **Close** to return to the previous screen.

Details were displayed, and your instrument is configured based on the settings you selected.

NOTE:

If no MAC address was discovered, go to the Ethernet setup tab, change the destination type to Unicast, and then re-discover the instruments.

Discovering network devices

The Network Discovery test is used to identify nodes and devices on the local network It is typically done to gain knowledge of accessible devices prior to analysis and debug. It provides information about what kinds of devices are available for access, and information about how the network is configured.

To discover network devices

Step1 If you haven't already done so, use the Test Menu to select the Traffic test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Toolkit** soft key, and then select the **Network Discovery** tool.

Step3 Select the **Settings** button, and then specify the following settings.

Setting	Description
Mode	Specify whether the discovery is active or passive.If testing layer 2, this cannot be changed, it is always passive
MAC Source Type	Specify the MAC address to use - the factory default or a user defined address.
User Defined MAC	If the MAC source is user defined address, specify the user defined MAC address
Source IP Type	Specify the source of the IP address (Static or DHCP). If testing layer 2, this item is not available.
Source IP	If the IP Type is Static, specify the local IP address.
Default Gateway	If the IP Type is Static, specify the local gateway.
Subnet Mask	If the IP Type is Static, specify the local subnet mask.
DNS Type	Indicates where to get the DNS address. If IP Type is Static, use Static; if DHCP, use Auto.
Primary DNS	If the DNS Type is Static, specify the IP address of the primary DNS server
Secondary DNS	If the DNS Type is Static, specify the IP address of the secondary DNS server

Step4 **Start** the discovery.

The test reports the discovered devices. This could include all or only a few of the following:

- Infrastructure:
  - IP Networks - Listing of subnets discovered and count of devices discovered per subnet.
  - Domains - Listing of domains discovered (NetBIOS) and count of devices discovered per domain.
  - VLANs - Listing of VLAN IDs discovered, priorities of the discovered VLANs, and count of devices per VLAN.
- Core
  - Routers - Listing of the IPs discovered and a list of the MACs discovered.
- Distribution
  - Switches - Listing of switches discovered and the services provided by the switch.
- Access
  - Hosts - Name of the devices as known to the DNS, the IP address of the device, MAC address of the device, and the name of the device as known to NetBIOS.
  - Servers - Name of the devices as known to the DNS, the IP address of the device, MAC address of the device, the name of the device as known to NetBIOS, and the services offered by the device.

Step5 *Optional.* To save the test results, select **Report** and then specify a file name for the report and the file format.

You have discovered network devices.

Programming JMEPs

JMEPs (JDSU Micro Ethernet Probes) can be programmed for applications such as:

- programming the IPv4 or IPv6 IP address of the JMEP so that in can be used to loop back Layer 3 Ethernet traffic to any T-BERD/MTS, HST or SmartClass device.
- programming the loop up and loop down functionality of the network and optical ports of a JMEP

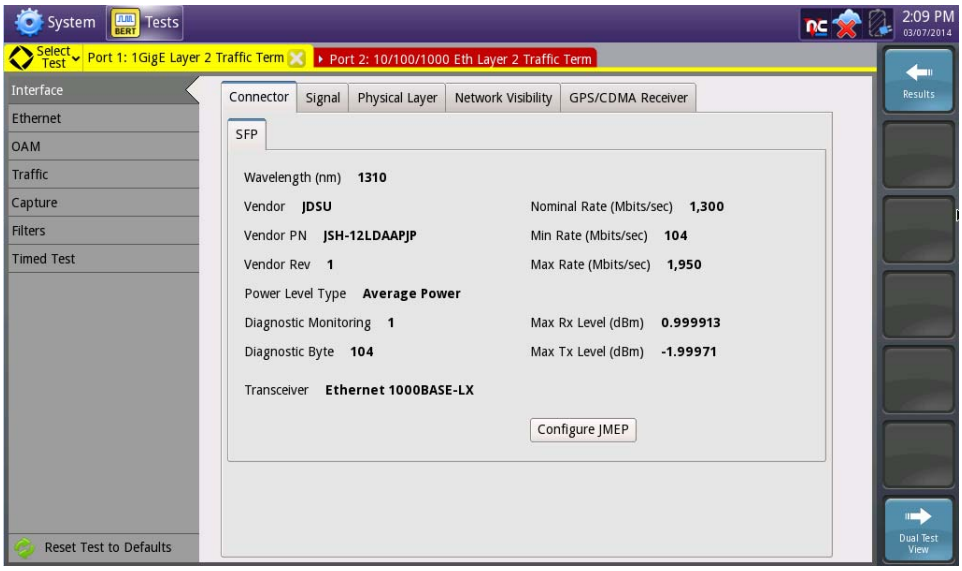
To program a JMEP

Step1 Launch an L2 or L3 1GigE application.

Step2 Insert a JMEP into the SFP slot associated with the application

Step3 Navigate to the SFP connector page (Setup>Interface>Connector).

If a valid JMEP is detected, a “Configure JMEP” button appears.



Step4 Select “Configure JMEP” to launch the SFProbe Programmer program.

Step5 Select **Read Device** to get a list of the current settings of the device.

Step6 To change any of the settings, do the following:

- **a** Find the field you wish to edit, and then click in the right column **Write Values**. Depending on the selected field, a dropdown menu appears or a keypad appears.
- **b** Select or enter the value for the field. For more information on the values for each field, refer to the SFProbe Programmer help or documentation.
- **c** Repeat steps a and b for each field, as needed.
- **d** Select **Write Device** to program the settings onto the device.

Step7 *Optional*. If you wish to set the values back to the factory settings, select Factory Settings.

Step8 Select the Exit icon in the upper right.

Protocol Analysis

The Protocol Analysis utility automates the capture/decode process by passively detecting a packet for a selected protocol and then providing the user relevant information decoded from the packet.

This utility detects and decodes port data in LAN networks configured using the Cisco Discovery Protocol (CDP) or the Link Layer Discovery Protocol (LLDP). Protocol Analysis can be used to recover the switch and port data supplied during configuration to determine port availability on a network.

To analyze protocol

Step1 If you haven't already done so, use the Test Menu to select a Traffic Monitor test application for the interface you are testing. Refer to Table 2 on page 26 for a list of layer 2 and layer 3 applications.

NOTE:

The Protocol Analysis utility is provided in all Layer 2 and Layer 3 Ethernet traffic monitoring applications from 10/100/1000 to 10GigE interfaces (10GigE WAN excluded).

Step2 Select the **Toolkit** soft key, and then select the **Protocol Analysis**.

Step3 Select the Protocol to Analyze **- CDP** or **LLDP**.

Step4 To initiate the protocol analysis click the **Start Analysis** button.

The utility displays the configured parameters of the ports analyzed:

– *CDP*:
  – Device Identifier - Name specified for the device containing the port.
  – Port Identifier - Name specified for the port.
  – VLAN ID - Name specified for the VLAN into which the port has been configured.
  – Source MAC address - MAC address of the device IP subnet address.
  – IP subnet address - IP subnet address into which the device containing the port has been configured.
– LLDP:
  – Chassis identifier - Name specified for the chassis containing the port.
  – Port identifier - Name specified for the port.
  – Time to Live - Duration of the LLDP advertisement value.
  – Source MAC (with optional VLAN identifier) - MAC address of the device IP subnet address and (optional) specified name for the VLAN into which the port has been configured.
  – Management IP address - The IP address for the management port of the device.
  – MAU Type - Medium Attachment Unit Type - The physical component type used to transmit/receive on the port identified.

Step5 *Optional.* To save the test results, select **Export Text File** and then accept the given filename or click **Rename** button and specify a file name for the report, to be saved in the Reports subdirectory, and select **OK** twice.

You have completed protocol analysis.

Layer 1 BER testing

When testing 1 Gigabit, 10 Gigabit LAN, 10 Gigabit WAN, or 100 Gigabit Ethernet service, you can generate and receive layer 1 test patterns, and monitor and analyze received signals.

NOTE: Changing BERT patterns

If you change a BERT pattern during the course of your test, be certain to press the **Restart** soft key to ensure that you regain pattern sync.

BER testing layer 1

Use the layer 1 BERT terminate application to generate and receive layer 1 test patterns.

NOTE:

For 10 Gigabit Ethernet patterns, refer to IEEE 802.3ae-2002, Sections 49.2.8, 49.2.12, and 52.9.1 for detailed descriptions of each pattern. For 1 Gigabit Ethernet MF, LF, and HF patterns, refer to the IEEE 802.3, 2000 Edition, Annex 26A. For 1 Gigabit Ethernet RDPAT, JTPAT, and SNPAT patterns, refer to the NCITS TR-25-1999 specifications.

To BER test layer 1

Step1 If you haven't already done so, use the Test Menu to select the Layer 1 BERT terminate application for the circuit you are testing. For PCS BERT testing go to step 4.

Step2 Select the **Setup** soft key.

Step3 Select the **Pattern** tab, and then do the following:

a Specify the **TX Pattern**.

b If you wish to do so, check the box for **Use same pattern for Tx and Rx** and then specify a Tx pattern. If using the Delay pattern, the box *should be checked* (Tx=Rx).

If the check box for **Use same pattern for Tx and Rx** is *not* checked, select an **Rx Pattern** and a **Tx Pattern**.

Step4 Connect the test instruments to the circuit.

Step5 On both instruments, if you are testing an optical interface, select the **Laser** button.

Step6 On both instruments, verify that the green Signal Present and Sync Acquired LEDs are illuminated. If using the Delay pattern, only the Signal Present LED appears (Sync Acquired is not used). For PCS BERT testing go to step 8.

Step7 On both instruments, do the following:

a If you are testing a 1GigE optical circuit, select the Actions tab, and then press the **Start BERT Pattern** button. This is not necessary if you are using the Delay pattern or testing a 10GigE LAN or WAN circuit.

b Verify that the green L1 Pattern Sync LED illuminates. If you are testing a 1GigE optical circuit, and the LED is not illuminated, stop transmitting the pattern from the other instrument, and then transmit it again. The LED will illuminate.

Step8 At a minimum, observe the test results in the following categories:

- Summary
- Error Stats

Layer 1 BER testing is complete.

When running the L1 BERT application, your LEDs may indicate that you have **L1 Pattern Sync** without word sync. The word sync status is indicated on your unit using a red **Sync Acquired** LED (if word sync was obtained, then lost), or an extinguished LED (if word sync was never obtained since starting your test). This is usually due to a temporary loss of signal or word sync when receiving an L1 pattern that does not contain Ethernet compliant link characters (for example, IDLE). To resolve this, stop transmitting the L1 pattern momentarily to allow the receiver to regain sync, and then begin transmitting the pattern again. The exception is when using the Delay using any pattern other than Delay.

If this occurs, be certain to determine why the signal or word sync was lost temporarily.

Monitoring layer 1 BER

Use the layer 1 BERT monitor application to analyze the received signal, and then pass the signal bit-for-bit through the unit's transmitter (if you select Connect Rx to Tx).

NOTE:

If you are monitoring traffic on an optical circuit, be certain to turn the laser on using the Laser button on the Main screen.

To monitor layer 1 BERT

Step1 Using the Test Menu, select the Layer 1 BERT monitor/through test application for the interface you are testing.For PCS BERT testing go to step 4.

Step2 To specify the BER pattern for the traffic you are monitoring, select the **Setup** soft key, select the **Pattern** tab, and then select the **Rx Pattern**.

Step3 Press **Results** to return to the Main screen.

Step4 Connect the module to the circuit.

Step5 If you are testing an optical interface, select the **Laser** button.

Step6 Verify that the green Signal Present LED is illuminated. For PCS BERT testing go to step 8.

Step7 Select **Connect Rx to Tx** to pass the received pattern through to the transmitter.

Step8 At a minimum, observe the test results in the following categories:

- Summary
- Error Stats

Monitoring layer 1 BERT is complete.

Link connectivity testing

Using the Link Connectivity Test, you can locate which port on the hub, switch, or router is being used. This is useful when one technician is troubleshooting and the test access port is in a different physical location than the switch.

CAUTION: LOSS OF DATA

This is an intrusive test. It temporarily brings the link down. This action disrupts signal and link. Please save any application results desired.

To test link connectivity (not applicable with 40G/100G High Speed Transport Module)

Step1 Connect the instrument to the circuit.

Step2 Verify that you are generating traffic or the laser has been turned on.

Step3 Select the **Toolkit** soft key, and then select the **Link Connectivity Test** tool.

The Link Connectivity Test window opens.

a Specify the desired Link Up and Link Down durations and the number of link toggles,

b Press the Start Toggling Link soft button to begin Link Connectivity testing.

Step4 The link connectivity test will run until the defined parameters of the test has been achieved or the Stop Toggling Link soft button has been pushed. Traffic may be started while link connectivity test is enabled. Frames will be sent while link is present and shall be reactivated when the test concludes.

Step5 Go to the location of the hub, switch, or router and observe the link activity LEDs. The port that is connected to the instrument will blink according to the parameters set in step 3.

Step6 This action disrupts signal and link. Please save any application results desired.

Layer 2 testing

Using the instrument, you can transmit, monitor, and analyze layer 2 Ethernet traffic. Step-by-step instructions are provided in this section for the following:

– “Specifying interface settings” on page 46
– “Specifying Ethernet frame settings” on page 49
– “Specifying Ethernet filter settings” on page 56
– “Specifying traffic load settings” on page 64
– “Transmitting and analyzing layer 2 traffic” on page 68
– “Transmitting and analyzing layer 2 patterns” on page 69
– “Monitoring layer 2 traffic” on page 70
– “Transmitting and analyzing layer 2 MPLS-TP, T-MPLS or MPLS traffic” on page 70
– “Using J-Proof to verify layer 2 transparency” on page 74



NOTE:

If during the course of testing you change the frame length (or settings that impact the calculated frame length) while the unit is already transmitting traffic, the unit resets your test results, but some residual frames of the old length may be counted because they are already in the traffic stream.

Specifying interface settings

Before you transmit traffic, you can specify interface settings which:

– Indicate which SFP jack you are using (if you are monitoring traffic on a 1 GigE circuit, and your unit is equipped with SFP jacks).
– Specify the transmitted wavelength (if you are monitoring traffic on an 10 Gigabit Ethernet circuit, and your unit is equipped with 850 nm, 1310 nm, and 1550 nm connectors).
– Turn flow control off to ignore pause frames sent to the instrument by its Ethernet link partner, or on if you want your unit to respond to received pause frames.
– Specify the pause quanta for transmitted pause frames. If you are specifying interface settings for an IP Video application, pause frames can not be transmitted; therefore, this setting does not appear on the Physical Layer sub-tab.
– Specify the speed and duplex settings for 10/100/1000 Ethernet traffic.

– Turn auto-negotiation for 10/100/1000 or 1 Gigabit Ethernet optical circuits on to tell the instrument to negotiate its capabilities with another Ethernet device before transmitting idle traffic. If you need to validate the auto-negotiation capabilities of the device you are negotiating with, you can change each of the module's default capabilities.



NOTE:

For 10/100/1000 Ethernet, if you turn auto-negotiation ON, and the Duplex setting is FULL, flow control is also ON by default. The module also advertises that it is capable of transmitting and receiving pause frames. If you turn auto-negotiation OFF, flow control is user-configurable.

If you turn auto-negotiation OFF, you must use a cross-over cable to connect to the circuit.

– Specify the source of the reference Signal Clock.

Internal - where synchronization with incoming signal is not necessary (default).

Recovered - from timing signals embedded in incoming signal (Sync-E).

External - stable reference signal input into connectors on the interface panel.

To specify interface settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the Interface tab.

Step3 View the Connector sub-tab. If multiple connectors are installed, select the unit to which the current setup applies.

Step4 Select the Signal sub-tab-

– If you have an older chassis, or if you selected a 10Gigabit Ethernet application, specify the wavelength. If your module only supports one wavelength (850 nm, 1310 nm or 1550 nm), the wavelength settings on the Main screen and Interface tab are disabled.

– If Tx Signal Clock is active (Enable Synchronous Ethernet checked on Physical Layer tab), select the Clock Source (not applicable to MSAM v1 or 5800 units) - **Internal, Recovered, or External.**

– For Internal mode, if latency compensation is required, enter the desired internal frequency offset.

Step5 Select the Physical Layer sub-tab, and then specify the following settings:

Interface	Settings
10/100/1000	– **Auto Negotiation.** If you want to negotiate capabilities with another switch, select **On**; otherwise, select **Off**. Auto Negotiation is always On when your unit is configured to test a 1000 BaseT interface. – **Pause Length (Quanta).** Select the field to enter the quanta to be carried by transmitted pause frames. To determine the pause duration, the receiving device performs the following calculation: **10 Mbps electrical:** Quanta x 51.2 ms **100 Mbps electrical:** Quanta x 5.12 ms **1000 Mbps electrical:** Quanta x 512 ns – **10BaseTX FDX/HDX.** **100BaseTX FDX/HDX** **1000BaseTX FDX/HDX** Select **Yes** if you want to advertise that the module is capable of full-duplex or half-duplex transmission for each rate; otherwise, select **No**. These settings only appear if auto negotiation is On. – **Flow Control.** If auto negotiation is OFF, select **On** if you want the module to adjust the transmitted bandwidth when it receives pause frames, or **Off** to ignore pause frames. – **Duplex.** If auto negotiation is off, specify Half or Full duplex transmission. – **Speed (Mbps).** If auto negotiation is off, specify **10** (10 Mbps) or **100** (100 Mbps) as the rate for the link. This setting only appears if auto negotiation is Off.
1 Gigabit	– **Auto Negotiation.** If you want to negotiate capabilities with another switch, select **On**; otherwise, select **Off**. – **FDX Capable/HDX Capable.** By default, the module advertises it is capable of full and half-duplex transmission (**Yes**). If you need to advertise that it is not capable, select **No**. This setting only appears if auto negotiation is On. – **Pause Capable.** By default, the module advertises it is capable of transmitting and interpreting received pause frames (**Both**). If you need to change the default capabilities, select **Neither**, **Tx Only**, or **Rx Only**. This setting only appears if auto negotiation is On. – **Flow Control.** Select **On** if you want the module to adjust the transmitted bandwidth when it receives pause frames, or **Off** to ignore pause frames. This setting only appears if auto negotiation is Off. – **Pause Length (Quanta).** Select the field to enter the quanta to be carried by transmitted pause frames. To determine the pause duration, the receiving device performs the following calculation: **1GigE optical:** Quanta x 512 ns
10 Gigabit LAN 10 Gigabit WAN	– **Flow Control.** Select **On** if you want the module to adjust the transmitted bandwidth when it receives pause frames, or **Off** to ignore pause frames. – **Pause Length (Quanta).** Select the field to enter the quanta to be carried by transmitted pause frames. To determine the pause duration, the receiving device performs the following calculation: **10GigE LAN optical:** Quanta x 51.2 ns

Step6 *Optional*. If you want to transmit an ID to identify all loop up/loop down frames originating from the module, select the Unit Identifier field, and then type the ID. The default ID is JDSU 6000.

Step7 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The interface settings are specified.

Specifying Ethernet frame settings

Before you transmit traffic, you can specify the frame characteristics of the traffic, such as the frame type (DIX, 802.3), control frame type (CDP, VTP, STP, or RSTP), encapsulation (VLAN, Q-in-Q, VPLS, or MPLS), and payload (Acterna test frames or BER patterns).

Things to consider

Consider the following before specifying the settings:

– CDP, VTP, STP, or RSTP headers. When configuring traffic with these headers, you can optionally specify EtherType settings; LLC, SNAP settings for 802.3 traffic are assigned automatically.

– Simulating traffic from a number of sources. If you would like to transmit traffic carrying a variety of source MAC addresses to simulate traffic from a number of sources, you can specify a beginning MAC address (or use the factory-assigned MAC address), and then indicate that the unit should automatically increment the address carried in each frame for a specific number of frames.

– ARP mode. If you are transmitting layer 3 traffic, you can enable ARP mode to determine the layer 2 destination MAC address of the destination or gateway router automatically, or you can disable ARP mode and then manually specify the destination MAC address. You can also indicate that the instrument should only ARP to devices on the same VLAN specified for transmitted traffic.

  You can also assign a user-defined source MAC address to your instrument to determine whether network problems originate with a particular address for an Ethernet device.

– ATP payloads carrying BERT patterns. Even when running software version 8.x, version 1 Transport Modules will not support ATP payloads carrying BERT patterns. Version 2 and Version 3 Transport Modules do support the payloads.

  40G/100G High Speed Transport Modules do not support ATP payload carrying BERT patterns. They only support ATP->Fill Byte.

– Changing BERT patterns or payload type. In order for a BERT analysis to be reliable, the test configuration must not change for the entire duration of the test. Changing any part of the configuration, including the pattern or source of the frames being analyzed (including changes in loopback) may result in momentary BERT bit errors and a pattern sync loss detected by the receiver after the traffic resumes.

  If you do experience bit errors and sync losses after changing the test configuration (including initiating loop up) and starting traffic, press the Restart soft key to clear the initial burst of errors. If you no longer make configuration changes, you can stop and start traffic without experiencing extraneous bit errors or sync losses. If you continue to see BERT bit errors after performing a test restart, this indicates a problem with the circuit under test.

  ATP Fill Pattern can be used if you do not wish to analyze BERT data.

– Byte sequence. The MSAM and Transport Module transmit the bytes in user defined patterns from left to right; the FST-2802 transmits the bytes in user defined patterns right to left. For example, a user defined hexadecimal pattern of 12345678 populates the frame as: 12345678.Using the same hexadecimal pattern, the FST-2802 would populate the frame as 78563412. Consider this when testing using the FST-2802.

Specifying the settings

To specify Ethernet frame settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the **Ethernet** tab.

Step3 In **Encapsulation**, select one of the following:

- **None**. If you do not want to encapsulate transmitted frames, select **None**.
- **VLAN.** If you want to transmit VLAN tagged frames, select VLAN, and then refer to "Configuring VLAN tagged traffic" on page 54.
- **Q-in-Q.** If you want to transmit VLAN stacked (Q-in-Q) frames, select **Q-in-Q**, and then refer to "Configuring Q-in-Q traffic" on page 55.
- **Stacked VLAN.** If you want to transmit stacked VLAN frames, select **Stacked VLAN**, and then refer to "Configuring stacked VLAN traffic" on page 55.
- **VPLS.** If you are testing on a VPLS network, *and you want to transmit traffic with a VPLS header*, select **VPLS**, and then refer to "Configuring VPLS traffic" on page 55.

  When you select VPLS encapsulation, the Frame Type label changes to SP Frame Type, and the L2 Transparency setting disappears.

NOTE: If you selected a Terminate application, and you want to filter received traffic using VPLS criteria, *you must select VPLS encapsulation for transmitted traffic*.

Step4 In Test Mode, specify the category of testing being done:

- **Traffic**. Standard mode that transmits unicast frames that satisfy the receiving unit's filter criteria.
- **J-Proof.** For verifying layer 2 transparency requiring loop back of all test frames including control frames and frames carrying a broadcast or multicast address (not applicable in multiple streams).
- **LBM Traffic.** For Loopback Message/Loopback Reply (LBM/LBR) frame analysis where the far-end unit (any equipment that responds to LBM messages) loops back any packet containing the LBM message.



NOTE:

If the LBM/LBR testing mode is required in RFC 2544 testing, it must be configured prior to initializing the RFC 2544 application.

LBM/LBR testing mode is not valid for any automatic scripting application other than RFC 2544.

Step5 In Frame Type, specify the type of frame you are transmitting (DIX, or 802.3).

Step6 If you are verifying layer 2 transparency, do the following:

a Turn L2 Transparency **On**.

b In Control Frame Type, select the frame type.



NOTE:

These settings are not applicable when testing 10 GigE WAN circuits.

Step7 If you selected a layer 2 application, in **Frame Size (Bytes)**, select one of the seven IEEE recommended frame lengths, Random, EMIX or enter a specific Jumbo, Undersized, or User Defined frame length. (If the payload is something other than Acterna with BERT payload, Undersized is available.)

NOTE

EMIX frame size is not available when configuring an Ethernet payload within OTU2e multiplexed signal.

If you selected Random or EMIX, use the **Configure** button to specify user-defined random frame sizes, including Jumbo, or select Reset to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations. EMIX also adds the EMIX Cycle Length field that controls how many frame entries are sent, in order, before cycling back to the first frame entry and repeating. To define the number of frame entries, enter a number between 1 and 8.

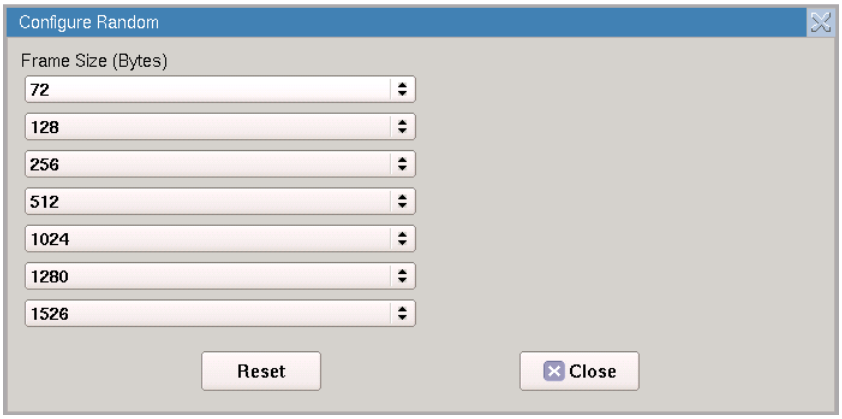


Figure 12 Configure Random Frame Size

Jumbo frames are not supported for 802.3 traffic per the 802.3 specification.

– If you are configuring layer 2 traffic, use the graphical display of a frame to specify the following:

Frame Label	Setting	Value
DA	Destination Type	Select the type corresponding to the Destination Address that will be inserted in the transmit frames: – **Unicast.** If you select Unicast, the least significant bit of the leftmost byte in the MAC address is forced to 0. – **Multicast.** If you select Multicast, the least significant bit of the leftmost byte in the MAC address is forced to 1. – **Broadcast** If you select Broadcast, the MAC address is automatically FFFFFFFFFFFF.
	Destination MAC	If you specified Unicast or Multicast as the destination type, enter the destination address using a 6 byte hexadecimal format.
	Loop Type	Select one of the following: – **Unicast.** The unit will issue a unicast message and loop-up the device with the Destination MAC address that you specified. – **Broadcast**. The unit will issue a broadcast hello message, and will then send a unicast loop-up to the first device on the circuit that responds to the hello.
SA	Source Type	Select **Factory Default** or **User Defined**.
	User MAC	If you specified User Defined, enter the unicast source MAC address using a 6 byte hexadecimal format.
	Auto Increment MAC	If you would like the unit to automatically increment the MAC address carried in each frame by one, select **Yes**.
	# MACs in Sequence	If you indicated that you would like the unit to increment the MAC addresses, specify the number of MACs in the sequence. The addresses will be assigned in succession, and will repeat after the number specified for the sequence is complete.
	Disable OoS Results	If you indicated that you would like the unit to increment the MAC addresses, any results derived from the out of sequence result (lost frames) will show “N/A” in the results display.
Type	EtherType	If Tx Payload is Acterna, specify desired Ethertype value from 0x0600-0xFFFF. Received ATP frames must have the same ethertype to be recognized as Acterna Test Packets.

Frame Label	Setting	Value
Data	TX Payload	Select from- **Acterna.** To transmit frames that contain a sequence number and time stamp so that lost frames, round trip delay, and jitter can be calculated, select **Acterna**. – **Acterna Payload Ver.** - Acterna Test Protocol (ATP) Version 2 and Version 3 handle time resolution differently, so ATPv3 provides higher resolution than ATPv2 for more precise RTD and packet jitter results. – **Acterna Fill Pattern**- these may be filled with any hexadecimal bytes, up to a total of 64 bytes. – **Delay Setup (MSAMv1 only)**- if you are measuring round trip delay, indicate whether you want to measure delay with a high degree of precision, or a low degree of precision. In most instances, you should select **High Precision - Low Delay**. See Table 8 on page 54 for Delay Measurement Topology on various platforms. **BERT.** To transmit frames with payloads filled with the BERT pattern you specify, select **BERT**, and then select a pattern. – Depending on the equipment being used, various pseudo-random and Fixed patterns are available. The pseudo-random patterns continue from one frame into the next. The fixed patterns restart each frame, such that the frame will always start with the beginning of the pattern. – If User Defined is an option and selected as the BERT Pattern, in the User Pattern field, specify the 32 bit fixed pattern that will be repeated in the payload. **Optic Latency Factor** This setting provides a means to compensate for significant intrinsic delays, especially when using certain types of pluggable optics affecting Frame Delay (latency) measurement results. In particular, if using the 40G/100G Transport Module, 100G LR4 CFP optics equipped with gearbox functionality have been shown to introduce delays in the range of 70 to 170 nanoseconds. Should this intrinsic delay be deemed significant, the Optic Latency factor allows compensation by specifying a value between 0 and 100 microseconds, with nanosecond granularity. This factor will be subtracted from latency calculations. To specify the Optic Latency Factor, do the following: **a** Run an RTD test with a very short fiber self-loop. **b** Enter the returned RTD value in the Optic Latency Factor field on the Setup page.

Table 8 Delay Measurement Topology

Delay Type	Payload Version	Platform	Rate	Maximum Distance(km)	Delay
Round Trip (RT)	High Precision ATPV3	CSAM 40G/100G Transport Module	100G	37,000 (RT)[a] 18,500 each way	189msec
			40G	94,000 (RT) 47,000each way	470msec
		MSAMv2, MTS 5800	10G	189,000 (RT)[a] 94,500 each way	0.9 sec
			1G	1,890,000 (RT)[a] 945,000 each way	9 sec
	High Precision ATPv2	CSAM 40G/100G Transport Module	100G	7,747,000 (RT) 3,873,500 each way	>10sec
			40G	19,000,000 (RT) 9,500,000 each way	>10sec
		MSAMv2, MTS 5800	10G	38,000,000 (RT) 19,000,000 each way	>10sec
			1G	380,000,000 (RT) 190,000,000 each way	>10sec
		MSAMv1	10G	75.500 (RT)[b] 37,750 each way	0.375 sec
			1G	755.000 (RT)[b] 377,500 each way	3.75sec
		Transport Module	10G	1,180[b]	5.9 msec
			1G	11,800[b]	59 msec
One-Way (using external GPS/CDMA reference)	High Precision ATPV3	MSAMv2, MTS 5800	10G	94,500	0.45 sec
			1G	945,000	4.7sec
	High Precision ATPv2	MSAMv1	10G	1,180	5.9 msec
			1G	11,800	59.1 msec

a. For longer distances use High Precision ATPv2
b. For longer distances use Low Precision ATPv2

Step1 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The frame settings for transmitted traffic are specified.

Configuring VLAN tagged traffic

To configure VLAN tagged traffic

Step1 After selecting VLAN as your encapsulation, on the graphic of the frame, select **VLAN**

Step2 Enter the VLAN ID transmitted in the VLAN ID field in a decimal format ranging from 0 to 4095.

Step3 In User Priority, select the priority (0 to 7) from the drop-down menu.

Step4 Do one of the following:

- If you are configuring traffic for a layer 2 application, return to "Specifying Ethernet frame settings".
- If you are configuring traffic for a layer 3 application, return to "Specifying transmitted IPv4 packet settings".

VLAN settings are specified.

Configuring Q-in-Q traffic

To configure Q-in-Q traffic

Step1 After selecting **Q-in-Q** as your encapsulation, on the graphic of the frame, select SVLAN, and then specify the SVLAN ID, SVLAN User Priority, DEI Bit, and SVLAN TPID for the service provider. You can now specify a User Defined TPID if you choose to.

Step2 Select CVLAN, and then specify the VLAN ID and User Priority for the customer's traffic.

Step3 Return to "Specifying Ethernet frame settings" for details on specifying the remaining settings.

Q-in-Q settings are specified.

Configuring stacked VLAN traffic

To configure stacked VLAN traffic

Step1 After selecting **Stacked VLAN** as your encapsulation, on the graphic of the frame, select VLAN Stack, and then specify the stack depth (number of VLANs).

Step2 For each VLAN, specify the SVLAN ID, SVLAN User Priority, DEI Bit, and SVLAN TPID for the service provider. You can now specify a User Defined TPID if you choose to.

Step3 Select CVLAN, and then specify the VLAN ID and User Priority for the customer's traffic.

Step4 Return to "Specifying Ethernet frame settings" for details on specifying the remaining settings.

Stacked VLAN settings are specified.

Configuring VPLS traffic

To configure VPLS traffic

Step1 After selecting **VPLS** as your encapsulation, on signal diagram, select **Tunnel Label**, and then specify the Tunnel ID (the label the network will use to route the traffic), the Tunnel Priority, and the Tunnel TTL value.

NOTE: VPLS settings are only available when configuring layer 2 test applications.

Step2 To specify a virtual circuit (VC) label for the transmitted traffic, select **VC Label**, and then specify the VC ID (the label the network will use to route the traffic on the channel to the appropriate interface), the VC Priority, and the VC TTL value.

Step3 To specify the customer destination address, source address, type, and payload, select **Data**, and then specify each of the settings.

Step4 Based on your settings, the unit automatically calculates and displays the service provider's overall frame size in the Calc. SP Frame Size field. Return to step – on page 52 of "Specifying Ethernet frame settings" for details on specifying the remaining settings.

VPLS settings are specified.

Configuring LBM Traffic

To configure LBM Traffic

Step1 After selecting LBM Traffic as the Test Mode (see step 4 in "Specifying the settings" on page 50), on the frame graphic, select **LBM.**

Step2 Specify the **Maintenance Domain Level** to which the transmitting unit belongs. If desired, also select the **Enable Sender TLV** checkbox to include the unit identifier (defined on the Network Visibility tab of the Interface setup page) in the header data.

LBM settings are specified.

Specifying Ethernet filter settings

Before transmitting traffic, you can specify settings that indicate the expected received payload and determine which frames or packets will pass through the filter and be counted in the test result categories for filtered traffic. For example, you can set up the filter to observe results for all traffic sent to a specific destination address. The filter settings may also impact other results.



NOTE:

During layer 2 BER testing, incoming frames must pass the filter to be analyzed for a BERT pattern. Local loopback is also only performed on frames that pass the filter. Use the filter to analyze BERT frames when non-test frames are present, such as spanning tree frames.

If you are transmitting Q-in-Q, VPLS, or MPLS encapsulated traffic, refer to:

– "Filtering traffic using Q-in-Q criteria" on page 58
– "Filtering traffic using VPLS criteria" on page 60
– "Filtering traffic using MPLS criteria" on page 61

To specify Ethernet filter settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the **Filters** tab. By default, a summary of all applicable filter settings appear (Ethernet, IP, and TCP/UDP).

Step3 In the panel on the left side of the tab, select **Basic**, then set the Filter Mode to **Detailed**.

Step4 To specify layer 2 filter settings, in the panel on the left side of the tab, select **Ethernet**, then specify the following:

a If you want to filter traffic based on the type of encapsulation used, specify the following:

Setting	Value
Encapsulation	Select one of the following: – **None**. The instrument will analyze only unencapsulated traffic. – **VLAN**. The instrument will analyze only VLAN encapsulated traffic for the parameters you specify. – **Q-in-Q**. The instrument will analyze only Q-in-Q encapsulated traffic for the parameters you specify. See "Filtering traffic using Q-in-Q criteria" on page 58. – **Stacked VLAN** (layer 2 applications only). The instrument will analyze only stacked VLAN encapsulated traffic for the parameters you specify. See "Filtering traffic using stacked VLAN criteria" on page 59. – **VPLS** (layer 2 applications only). The instrument will analyze only VPLS encapsulated traffic for the parameters you specify. See "Filtering traffic using VPLS criteria" on page 60. – **MPLS** (layer 3 applications only). The instrument will analyze only VPLS encapsulated traffic for the parameters you specify. See "Filtering traffic using MPLS criteria" on page 61. – **Don't Care**. The instrument will analyze traffic satisfying all other filter criteria regardless of encapsulation.
VLAN	If you specified VLAN as the encapsulation type, on the graphic display of the frame, select VLAN, and then specify the VLAN ID carried in the filtered traffic.
User Priority	If you specified VLAN as the encapsulation type, and you want to filter for traffic with a specific user priority, specify the priority, or select **Don't Care**.

b In Frame Type, specify one of the following:

Frame Type	Description
DIX	To analyze DIX frames only, select DIX.
EtherType	If you specified DIX as the frame type, specify the Ethertype by selecting the Type field on the graphic of the frame. If you do not specify the EtherType, the module will filter the traffic for DIX frames with the currently specified EtherType value.
802.3	To analyze 802.3 frames only, select 802.3.
Data Length (bytes)	If you specified 802.3 as the frame type, specify the data length by selecting the Length field on the graphic of the frame. If you do not specify the length, the module will filter the traffic for 802.3 frames with the currently specified length.
Don't Care	If you want to analyze both DIX and 802.3 VLAN or Q-in-Q encapsulated traffic, select **Don't Care**. You must specify a frame type if you are filtering unencapsulated traffic.

c If you want the unit to filter for traffic carrying a particular destination address, on the graphic of the frame, select **DA**, and then specify the following:

Setting	Value
Destination Type	If you want to analyze traffic with a specific type of destination address, select one of the following: – Unicast – Multicast – Broadcast Otherwise, select Don't Care to analyze traffic with any type of destination address.
Destination MAC	If you are filtering traffic for a specific Unicast or Multicast destination address, specify the address carried in the traffic that you want to analyze.

d If you want to filter traffic for a particular source address, on the graphic of the frame, select **SA**, and then specify the following:

Setting	Value
Source Type	If you want to analyze traffic with a Unicast source address, select **Unicast**; otherwise, select **Don't Care** to analyze traffic with any type of destination address.
Default MAC	If you are filtering traffic for a specific Unicast source address, specify the address carried in the traffic that you want to analyze.

Step5 To specify additional filter settings, see:

– "Filtering traffic using Q-in-Q criteria" on page 58
– "Filtering traffic using stacked VLAN criteria" on page 59
– "Filtering traffic using VPLS criteria" on page 60
– "Filtering traffic using MPLS criteria" on page 61
– "Filtering traffic using byte pattern criteria" on page 62
– "Filtering traffic using payload criteria" on page 63

Step6 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The Ethernet filter settings are specified.

Filtering traffic using Q-in-Q criteria

If your instrument is configured to transmit Q-in-Q encapsulated traffic, you can filter received traffic using Q-in-Q criteria.

To filter traffic using Q-in-Q criteria

Step1 If you haven't already done so, use the Test Menu to select the layer 2 or layer 3 test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for lists of applications.

Step2 Select the **Setup** soft key, and then select the Ethernet tab. Verify that Q-in-Q is specified as the encapsulation.

Step3 Select the **Filters** tab. In the panel on the left side of the tab, select **Ethernet**, then specify the following:

a On the graphic of the frame, select **SVLAN**, and then specify the following:

Setting	Value
SVLAN ID	Specify the SVLAN ID carried in the filtered traffic.
SVLAN User Priority	If you want to filter traffic for a specific user priority, specify the priority; otherwise, select **Don't Care**.
SVLAN DEI Bit	If you want to filter traffic for a specific DEI Bit, specify the bit value; otherwise, select **Don't Care**.
SVLAN TPID (hex)	Specify the TPID carried in the filtered traffic. If you are transmitting traffic with a user defined TPID, your instrument will automatically use the TPID that you specified in the User SVLAN TPID (hex) field. **NOTE:** If you want to filter on a user-defined TPID, you must also enter that TPID on the RX Payload/TPID setup page.

b On the graphic of the frame, select **CVLAN**, and then specify the following:

Setting	Value
Specify VLAN ID	If you specified Q-in-Q as the encapsulation type, and you want to filter traffic for a specific CVLAN, select **Yes**; otherwise, select **Don't Care**.
VLAN ID	If you specified Q-in-Q as the encapsulation type, and you specified indicated that you want to filter traffic for a particular CVLAN, specify the VLAN ID carried in the filtered traffic.
User Priority	If you specified Q-in-Q as the encapsulation type, and you specified indicated that you want to filter traffic for a particular CVLAN, specify the User Priority carried in the filtered traffic.

Step4 If you want to analyze/detect frames carrying User Defined SVLAN TPID as Q-in-Q traffic, you have to specify the expected User Defined TPID value(s) on the Filters->Rx->TPID page. The TPID values on this page are used to recognize Q-in-Q traffic with User Defined TPID. If you want to analyze/detect Q-in-Q traffic carrying the same TPID that you specified for transmitted traffic, check the box for Use Tx User SVLAN TPID.

Step5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The Q-in-Q filter settings are specified.

Filtering traffic using stacked VLAN criteria

If your instrument is configured to transmit stacked VLAN encapsulated traffic, you can filter received traffic using stacked VLAN criteria.

To filter traffic using stacked VLAN criteria

Step1 If you haven't already done so, use the Test Menu to select the layer 2 test application for the interface you are testing. Refer to Table 2 on page 26 for lists of applications.

Step2 Select the **Setup** soft key, and then select the Ethernet tab. Verify that Stacked VLAN is specified as the encapsulation.

Step3 Select the **Filters** tab. In the panel on the left side of the tab, select **Ethernet**, then specify the following:

a On the graphic of the frame, select **SVLAN**, and then specify the following:

Setting	Value
SVLAN ID	Specify the SVLAN ID carried in the filtered traffic.
SVLAN User Priority	If you want to filter traffic for a specific user priority, specify the priority; otherwise, select **Don't Care**.
SVLAN DEI Bit	If you want to filter traffic for a specific DEI Bit, specify the bit value; otherwise, select **Don't Care**.
SVLAN TPID (hex)	Specify the TPID carried in the filtered traffic. If you are transmitting traffic with a user defined TPID, your instrument will automatically use the TPID that you specified in the User SVLAN TPID (hex) field.

b On the graphic of the frame, select **CVLAN**, and then specify the following:

Setting	Value
Specify VLAN ID	If you specified stacked VLAN as the encapsulation type, and you want to filter traffic for a specific CVLAN, select **Yes**; otherwise, select **Don't Care**.
VLAN ID	If you specified stacked VLAN as the encapsulation type, and you specified indicated that you want to filter traffic for a particular CVLAN, specify the VLAN ID carried in the filtered traffic.
User Priority	If you specified stacked VLAN as the encapsulation type, and you specified indicated that you want to filter traffic for a particular CVLAN, specify the User Priority carried in the filtered traffic.

Step4 If you want to analyze/detect frames carrying User Defined SVLAN TPID as Stacked VLAN traffic, you have to specify the expected User Defined TPID value(s) on the Filters->Rx->TPID page. The TPID values on this page are used to recognize Stacked VLAN traffic with User Defined TPID. If you want to analyze/detect Stacked VLAN traffic carrying the same TPID that you specified for transmitted traffic, check the box for Use Tx User SVLAN TPID.

Step5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The stacked VLAN filter settings are specified.

Filtering traffic using VPLS criteria

If your unit is configured to transmit VPLS encapsulated traffic, you can filter received traffic using VPLS criteria.

To filter traffic using VPLS header criteria

Step1 If you haven't already done so, use the Test Menu to select the layer 2 test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for lists of layer 2 applications.

Step2 Select the **Setup** soft key, and then select the Ethernet tab. Verify that VPLS is specified as the encapsulation.

Step3 Select the **Filters** tab. In the panel on the left side of the tab, select **Ethernet**, then specify the following:

a On the graphic of the frame, select **Tunnel Label**, and then specify the following:

Setting	Value
Tunnel Label	If you want to filter received traffic based on the tunnel label, set the Tunnel Label filter to **Yes**; otherwise, select **Don't Care**.
Tunnel Label	If you indicated that you want to filter traffic for a specific tunnel, enter the label.
Tunnel Priority	If you want to filter received traffic based on the tunnel priority, set the Tunnel ID Filter to **Yes**; otherwise, select **Don't Care**.
Tunnel Priority	If you indicated that you want to filter traffic for a specific tunnel, select the priority number.

b If you want to filter received traffic using virtual circuit criteria, select **VC Label**, and then specify the following:

Setting	Value
VC Label	If you want to filter received traffic based on the tunnel ID, set the VC Label to **Yes**; otherwise, select **Don't Care**.
VC Label	If you indicated that you want to filter traffic for a specific label, enter the label.
VC Priority	If you want to filter received traffic based on the virtual channel priority, set the priority filter to **Yes**; otherwise, select **Don't Care**.
VC Priority	If you indicated that you want to filter traffic for a specific virtual channel priority, select the priority number.

Step4 Return to "Specifying Ethernet filter settings" to verify or specify additional filter settings.

VPLS filter criteria is specified.

Filtering traffic using MPLS criteria

To filter traffic using MPLS header criteria

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for lists of layer 3 applications.

Step2 Select the Setup soft key, and then select the **Ethernet** tab. Verify that the encapsulation is set to MPLS.

Step3 Select the **Filters** tab. In the panel on the left side of the tab, select **Ethernet**, then specify the following:

a Above the graphic of the frame, set the MPLS Type Filter to **Enable**.

b In EtherType, select **MPLS Unicast** or **MPLS Multicast**.

c On the graphic of the frame, select **MPLS Label 1**, and then specify the following:

Setting	Value
MPLS1 Label	If you want to filter received traffic based on the label, set the filter to **Yes**; otherwise, select **Don't Care**.
MPLS1 Label	If you indicated that you want to filter traffic for a specific label, enter the label.
MPLS1 Priority	If you want to filter received traffic based on the priority, set the filter to **Yes**; otherwise, select **Don't Care**.
MPLS1 Priority	If you indicated that you want to filter traffic for a specific priority, select the priority number.

Step4 If you want to specify additional criteria for MPLS2, on the graphic of the frame, select MPLS Label 2, then repeat step 3.

Step5 Return to "Specifying Ethernet filter settings" to verify or specify additional filter settings.

MPLS filter criteria is specified.

Filtering traffic using byte pattern criteria

If you want to do so, you can specify criteria to filter based on the byte pattern.

To filter traffic using byte pattern criteria

Step1 If you haven't already done so, use the Test Menu to select the layer 2 test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for lists of layer 2 applications.

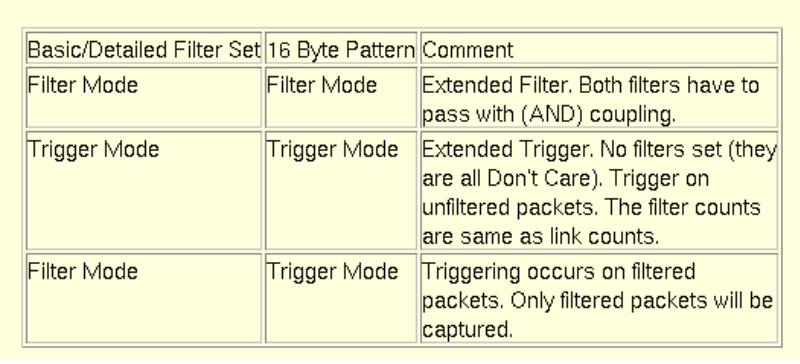
Step2 Select the **Capture** tab, and then set **Capture** to **Enable** and set **Use Filters as** to **Filter**.

Step3 Select the **Filters** tab, and then specify the following:

a In the panel on the left side of the tab, select **Summary**, and then select **Clear All Filters** to clear any previous filter settings.

b In the panel on the left side of the tab, select **Byte Pattern**, and then set **Use Byte Pattern as** to **Filter**.

Figure 13 explains the different filter and trigger modes.(You can find this table by clicking the ? next to Use Byte Pattern as).



Basic/Detailed Filter Set	16 Byte Pattern	Comment
Filter Mode	Filter Mode	Extended Filter. Both filters have to pass with (AND) coupling.
Trigger Mode	Trigger Mode	Extended Trigger. No filters set (they are all Don't Care). Trigger on unfiltered packets. The filter counts are same as link counts.
Filter Mode	Trigger Mode	Triggering occurs on filtered packets. Only filtered packets will be captured.

Figure 13 Filter and trigger modes

c Specify the following:

Setting	Value
Match Method	Select how to match the pattern: **Fixed offset** (match the pattern at the specified **Pattern Offset**) or **Sliding Window** (match the pattern anywhere in the header).
Byte Pattern	In the graphic of the Byte Pattern, click on the individual bit and set the hex pattern and the mask. The mask specifies whether to match both bits (FF) one bit (0F or F0), or don't care (00).

Filtering traffic using payload criteria

You can filter traffic using payload criteria, or you can turn payload analysis off entirely.

To specify payload filter settings

Step1 In the panel on the left side of the tab, select **Rx Payload**, then specify the following:

Setting	Value
Payload Analysis	Specify one of the following: – **Off.** If you want the module to monitor and analyze live Ethernet traffic by suppressing lost frames (LF) or BERT errors in their associated result counts and as triggers for LEDs during payload analysis, select Off. – **On.** If you want to analyze traffic carrying a particular BERT pattern, select On.
Use Tx BERT settings	Specify one of the following: – If you want the module to monitor and analyze traffic carrying a different BERT pattern than the one specified for transmitted traffic, un-check the box. – If you want to analyze traffic carrying the same BERT pattern carried in transmitted traffic, check the box.
Rx Payload (Payload Analysis On, and Use Tx BERT settings unchecked)	Specify **Acterna** or **BERT**.
Rx BERT Pattern Payload Analysis On, and Use Tx BERT settings unchecked)	If you unchecked Use Tx BERT settings, specify the BERT pattern carried in the filtered traffic.

Payload filter criteria is specified.

Specifying traffic load settings

Before transmitting traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty or Ramp). The settings vary depending on the type of load. When configuring a load, you can specify the bandwidth of the transmitted traffic in 0.001% increments.

NOTE:

If you configure the instrument to transmit a bursty or ramped load of 100%, the module is designed to transmit slightly less than 100% traffic (99.996% for 10 Gigabit Ethernet, 99.90% for 1 Gigabit Ethernet, and 99.90% for 10/100/1000 Ethernet) as a safeguard against overrunning network elements that can not support 100%. If you are certain the elements can support true 100% traffic, select the Allow flooding check box when configuring the Constant load.

Transmitting a constant load

With a **constant** load, the module transmits frames continuously with a fixed bandwidth utilization. You can specify the load as a percent or a bit rate. See Figure 14.

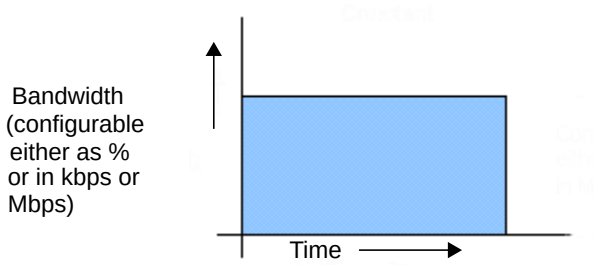


Figure 14 Constant traffic

When you setup a constant traffic load, if you are running a standard Ethernet application, you can specify the bandwidth as a percentage of the line rate (%BW) or at a specific bit rate. The bit rate can be specified in total kbps or Mbps.

To configure the module to transmit a constant load of traffic

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the Traffic tab.

Step3 In Load Type, select **Constant**.

Step4 In Load Unit, select one of the following:

- **Percent**. If you select Percent, in **Load %**, enter the duty cycle as a percentage.
- **Bit Rate**. If you select Bit Rate, in **Load (Mbps)** or **Load (kbps)** enter the bit rate in Mbps or kbps.
- **Frames Per Second**. Valid only for Constant in Non-Streams Apps; Valid for Constant and Ramp in Streams.

Step5 Select the **Allow flooding** check box to transmit true 100% load in those circuits that can certainly handle the signal.

Step6 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The module is configured to transmit a constant rate of traffic.

Transmitting a bursty load

With a **bursty** load, the module transmits frames at 100% bandwidth for a specific time interval, followed by no frame transmissions during the specified gap interval. See Figure 15.

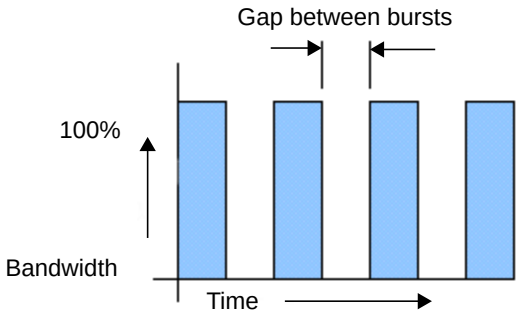


Figure 15 Bursty traffic

When you configure bursty traffic, if you are running a standard Ethernet application, you can specify the burst load as a percentage of the duty cycle, or by specifying the burst and gap intervals in units of time, bytes and Information Rate (IR). If you specify the burst load as a percentage of the duty cycle, and then specify the number of frames per burst, the module automatically calculates the burst gap.

NOTE:

If you configure a bursty load of traffic with a low percentage of the line rate (duty cycle) and a large number of frames per bust, it may appear that traffic transmission has stopped periodically. This is because the calculated interval (gap) between bursts will be longer. A higher percentage of the line rate and a lower number of frames per burst results in a shorter interval (gap).

To configure the module to transmit bursts of traffic

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the Traffic tab.

Step3 In Load Type, select **Burst**.

Step4 In Load Unit, select one of the following:

- **Bytes and Information Rate**. Proceed to step 5.
- **Burst Time and Information Rate**. Proceed to step 5.
- **Gap Time and Information Rate.** Proceed to step 5.
- **Bytes and Gap Time**. Proceed to step 5.
- **Burst Time and Gap Time**. Proceed to step 5.
- **Frames and Duty Cycle**. Proceed to step 6.

Step5 If you selected any of the combinations of Time, Rates and Byte, the following parameters may need to be set:



NOTE

Values may be automatically normalized (rounded to nearest appropriate values) from values entered.

a **Information Rate**. Enter the average throughput rate in Mbps up to the maximum rate of the interface (layer 2 only).

b **Burst KBytes**. Enter the number of Kbytes of data desired to be transmitted in each burst of traffic.

c **Burst Time**. Enter the amount of time that each burst of traffic should be transmitted (will round to the nearest frame transmit time).

d **Time Unit.** Select unit for time entry - **sec**, **msec**, **usec** or **nsec.**

e **Gap/Idle Time.** Enter the amount of time between each burst. The valid range for this setting adjusts depending on the Burst Time that is entered, to ensure that the duty cycle is at least 1% in 0.001% intervals (will round to the nearest 0.001%).

The following parameters may be displayed as a result of the above selections-

f **Bit Rate** (calculated). Bits/Time Unit from Burst average throughput rate (will round kb down to the nearest frame size).

g **Actual KBytes** (calculated)**.** Actual value of bytes/burst. Values above the line rate can not be entered.

Step6 If you selected Frames and Duty Cycle as the load unit, set the following:

a **Duty Cycle (%)**. Enter the percentage of the line rate (the duty cycle) during which traffic will be transmitted in the burst, from 0.001 - 100%.

b **Frames/Burst Time**. Select a predefined value, or User-Defined, for the number of frames that are to be included in each burst.

c **User Burst Size**. If User-Defined is specified for Frames/Burst, define the User Burst size, 1- 65535 frames.

Step7 Specify the burst type for the traffic:

– **Fixed**. Sends a fixed number of bursts and then stops. If you select Fixed, enter the number of bursts.

– **Continuous**. Sends bursts continuously.

Step8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The module is configured to transmit bursts of traffic.

Transmitting a ramped load

With a **ramped** load, the module automatically increases the load by a percentage of bandwidth (specified as the load step) at a particular time interval (specified as the time step). The process is repeated, allowing you to easily verify the maximum throughput of a link. See Figure 16.

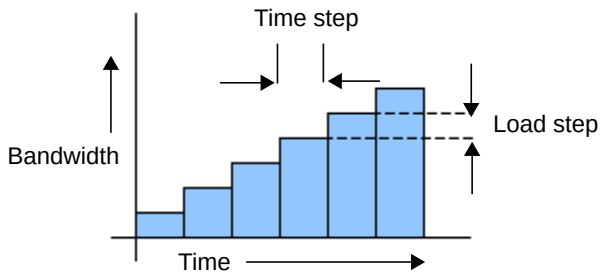


Figure 16 Ramped traffic

You can also specify criteria to tell the module to stop ramping if an error (or errors) occurs in a load step.

NOTE:

When configuring a ramped load of traffic for a particular stream (when running a multiple streams application), the triggers for stopping the ramp *are not available*.

To configure the module to transmit a ramped load of traffic

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the Traffic tab.

Step3 In Load Type, select **Ramp**, and then specify the following settings:

a **Time Step (sec)**. Enter the time step in seconds.

b **Load Step.** Enter the load step as a **Percentage** of the total bandwidth or in **fps** (streams application only)**.**

c **Frames Per Second (fps).** Applicable to streams application only**.**

Step4 *Optional*. If you want to stop the ramp from incrementing when certain errors occur, under Stop Load Increments, specify the following:

– **Errored Frames**. If you want to stop incrementing the load if FCS errored frames are detected, select **Yes**, and then enter the number of errored frames that must be detected to stop the ramp.

– **Dropped Frames**. If you want to stop incrementing the load if dropped frames are detected, select **Yes**, and then enter the number of dropped frames that must be detected to stop the ramp.

NOTE:

Acterna frames carry a sequence number which the unit uses to determine whether frames were dropped; therefore, you must configure your unit to transmit an Acterna payload, turn payload analysis on, and loop the far-end device back to the traffic originating unit.

– **Pause Frames**. If you want to stop incrementing the load if pause frames are detected, select **Yes**, and then enter the number of pause frames that must be detected to stop the ramp.

Step5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The module is configured to transmit ramped traffic.

Transmitting and analyzing layer 2 traffic

Before you transmit layer 2 traffic, you must specify:

– Interface settings (see “Specifying interface settings” on page 46).
– Frame characteristics for the transmitted traffic (see “Specifying Ethernet frame settings” on page 49).
– Frame characteristics used to filter received traffic (see “Specifying Ethernet filter settings” on page 56).
– Traffic load settings (see “Specifying traffic load settings” on page 64).

After you specify the layer 2 settings, you are ready to transmit and analyze the layer 2 traffic.



NOTE: Layer 2 BERT testing

Layer 2 BERT patterns carried in a BERT payload are not compatible with BERT patterns carried in an ATP payload. When testing using two instruments, be certain to configure both using the same payload type and BERT pattern.

To transmit and analyze layer 2 traffic

Step1 If you haven’t already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 applications.

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see “Specifying interface settings” on page 46).

Step3 Select the **Ethernet** tab to specify settings that define the frame characteristics of the transmitted traffic (see “Specifying Ethernet frame settings” on page 49).

Step4 Select the **Ethernet Filter** tab to specify settings that filter the received traffic based on specified frame characteristics (see “Specifying Ethernet filter settings” on page 56).

Step5 Select the **Traffic** tab to specify the type of load the unit will transmit (see “Specifying traffic load settings” on page 64).

Step6 Press **Results** to return to the Main screen.

Step7 Connect the module to the circuit.

Step8 If you are testing an optical interface, select the **Laser** button.

Step9 Select **Start Traffic** to transmit traffic over the circuit.

Step10 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step11 At a minimum, observe the summary, link statistics and counts, filter statistics and counts, error statistics, and layer 2 BERT statistics results.

You have analyzed layer 2 traffic.

Transmitting and analyzing layer 2 patterns

Using the instrument, you can stress the jitter and noise characteristics of 1 Gigabit components and systems by transmitting continuous random test patterns (CRPAT), continuous jitter test patterns (CJPAT), and the compliant supply noise pattern (CSPAT). These patterns are always transmitted automatically when you turn the laser on.

NOTE:

You must run pattern tests using an end-to-end configuration at all times. These patterns are designed to test physical layer networks. By definition, these framed patterns populate the Ethernet header with invalid address information; therefore, these frames will not traverse a layer 2, switched network.

For the same reason, if the pattern frames are transmitted to a far-end Transport Module that is looped-up, the far-end Transport Module tries to swap the source address and destination address for the pattern frames. As a result, the patterns received by the near-end Transport Module are modified, and the results are not valid.

To transmit a pattern

Step1 If you haven't already done so, use the Test Menu to select the Layer 2 Patterns test application for the 1GigE Optical interface.

Step2 Select the **Setup** soft key. The Setup tab appears.

Step3 Select a pattern:

To…	Select…
Emulate a worst case scenario for deterministic jitter by transmitting frames with a broad spectral content.	**CRPAT**
Stress the timing margins in the received eye by exposing the data sampling circuits to large systematic phase jumps.	**CJPAT**
Emulate a worst case scenario for power supply noise within network transceivers.	**CSPAT**

Step4 Press **Results** to return to the Main screen.

Step5 Connect the module to the circuit.

Step6 If you are testing an optical interface, select the **Laser** button.

Step7 Verify that the green SIGNAL LED is illuminated.

Step8 Select **Start Pattern** to transmit the pattern over the circuit.

Step9 At a minimum, observe the summary and pattern statistic test results.

You have transmitted layer 2 patterns.

Monitoring layer 2 traffic

Use the layer 2 traffic monitor application whenever you want to analyze the received signal. You can also pass the signal bit-for-bit through to the unit's transmitter if you select Connect Rx to Tx. When you configure your test, you can specify settings that indicate the expected received payload and determine which frames will pass through the receive filter and be counted in the test result categories for filtered layer 2 traffic. The settings may also impact other results.

NOTE:

You must turn the laser on using the associated button to pass the signal through the unit's transmitter.

To monitor layer 2 traffic

Step1 Use the Test Menu to do one of the following:

– Select the layer 2 monitor test application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Select the **Setup** soft key, and then select the **Ethernet Filter** tab. Do one of the following:

– If you are running a standard Ethernet test application, specify the filter settings for the traffic you want to monitor (see "Specifying Ethernet filter settings" on page 56).

– If you are monitoring VPLS encapsulated traffic, specify the VPLS filter settings (see "Filtering traffic using VPLS criteria" on page 60).

Step3 Press **Results** to return to the Main screen.

Step4 Connect the module to the circuit.

Step5 If you are testing an optical interface, select the **Laser** button.

Step6 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step7 Select **Connect Rx to Tx** (for line loopbacks).

Step8 At a minimum, observe the summary, link statistics and counts, filter statistics and counts, error statistics, and layer 2 BERT statistics results.

Layer 2 traffic is monitored.

Transmitting and analyzing layer 2 MPLS-TP, T-MPLS or MPLS traffic

You can use the instrument to send and receive MPLS OAM messages or generate Ethernet traffic on a specific pseudo-wire inside a specific tunnel and analyze any MPLS-TP (ITU-T G.8113.1), T-MPLS (ITU-T G.8114),or MPLS (ITU Y.1711) traffic present on the Ethernet link.

About MPLS-TP

The differences between MPLS, T-MPLS OAM and MPLS-TP OAM are:

– MPLS and T-MPLS OAM uses the reserved Label 14 as the identifier and MPLS-TP uses the label 13 together with Associated Channel Header (ACH).

– T-MPLS and MPLS-TP can use Loop-Back Message and Loop-Back Reply (LEBM/LBR) while MPLS must use Continuity Verification (CV).

However, MPLS, T-MPLS and MPLS-TP OAMs all support multiple layers: section layer, tunnel/trunk layer or label switched path (LSP), and pseudo wire (PW) layer or virtual circuit (VC).

MPLS-TP is a connection oriented packet-switched transport technology. The main features of MPLS-TP are:

– Connection oriented
– Subset of MPLS (without IP functionality)
– Packet-based service support via point-to-point connection
– No dynamic control protocol
– Simplified data plane and forwarding
– End-to-end OAM
– Protection switching

MPLS-TP provides transport service using pseudo wire emulation edge-to-edge (PWE3) technology.

Figure 17 summarizes the evolution of MPLS-TP from MPLS via T-MPLS.

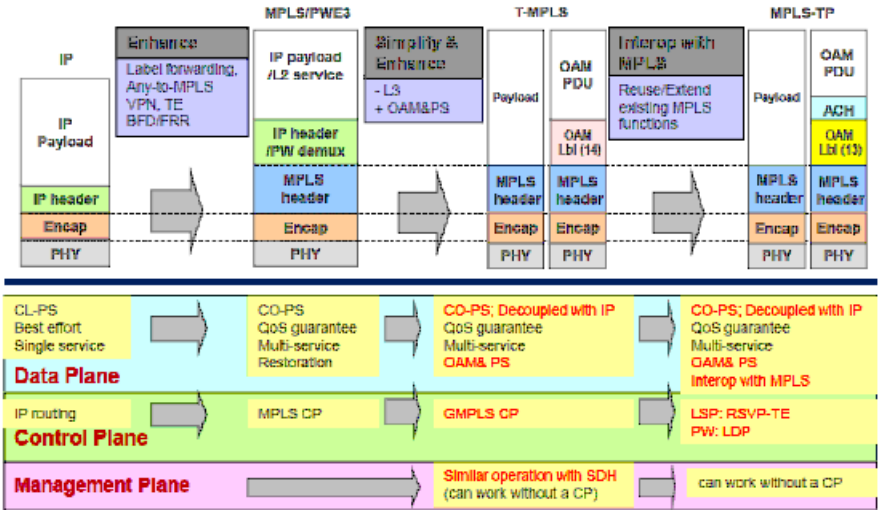


Figure 17 MPLS-TP evolution

Transmitting and analyzing MPLS-TP traffic

You can use the instrument to send and receive MPLS-TP OAM messages or generate Ethernet traffic on a specific pseudo-wire inside a specific tunnel and analyze any MPLS-TP traffic present on the Ethernet link.

To transmit and analyze L2 MPLS-TP traffic

Step1 If you haven't already done so, use the Test Menu to select the L2 MPLS-TP application for the interface you are testing. Refer to Table 4 on page 27 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **Ethernet** tab.

Step3 Specify the Service Provider Frame settings:

Encapsulation - **None** or **VLAN**

Frame Type - **DIX** or **802.3**

Control Word - specify (**ON**/**OFF**) whether an optional control word (fixed to all zeroes) is inserted before the payload.

For more information on the settings, see "Specifying Ethernet frame settings" on page 49

Step4 If VLAN was the encapsulation method selected, select the **VLAN** field on the image of the outgoing frame at the bottom of the page. Define the **VLANID** and the **User Pri(ority)**.

NOTE: Only one VLAN is supported.

Step5 Select the **OAM** tab, and then do the following:

a In the options list on the left side of the tab, select **Common Header** and then specify the settings:

Setting	Description
Type	Specifies the type of OAM transport service to be used: MPLS-TP, T-MPLS or MPLS.
Layer	Specifies the layer that OAM is operating on: PW, LSP, or Section. PW is only available if the *Control Word* field is set to **ON** on the Ethernet setup tab.
Label	Indicates the OAM encoding type, in label 13 (GAL) or label 14 (OAL).
ACH Channel Type	Specifies the channel type field in the associated channel header (ACH). Only appears if the Label Type is label 13.
Traffic Class	Specifies the traffic class field in the generic associated channel label (GAL). Only appears if the Label Type is label 13 and if using the Section or LSP layer.
TTL	Specifies the time to live (TTL) field. If the Label Type is label 13, this only appears if using Section or LSP layer. For label 14, it is always available. Per the y.17tom specification, this setting is applicable when LBM/LBR is enabled. If LBM/LBR is not enabled, this field is fixed to 1, even if set to something else.

b In the options list on the left side of the tab, select **CCM** (except when Y.1711(MPLS) was selected for type) and then specify the settings:

Setting	Description
Continuity Checking	Specifies whether to transmit/receive CCM messages.
LOC threshold	Specifies the number of messages required to reach the LOC threshold.
CCM Rate	Specifies the rate at which CCM frames are transmitted and the rate at which they are expected to be received.
MEG End Point ID	Specifies the local and peer MEG End Point ID.
Maintenance Domain Level	Specifies the Maintenance Domain Level.
Specify Domain ID	Indicates whether the Domain ID needs to be specified.as part of the Maintenance Association ID.
Maintenance Association ID	Specifies the Maintenance Association.

c In the options list on the left side of the tab, select **AIS** (except when Y.1711(MPLS) was selected for type), and then specify the settings:

Setting	Description
AIS State	Specifies whether to enable AIS.
Maintenance Domain Level	Specifies the Maintenance Domain Level.
AIS Rate	Specifies the rate at which AIS indications are sent. It is fixed to 1 second if the Label type is Label 14 (OAL).

d In the options list on the left side of the tab, select **LBM/LBR** (except when Y.1711(MPLS) was selected for type) and then specify the settings.

Setting	Description
LBM/LBR (ping)	Specifies whether to transmit/receive LBM/LBR messages.
Maintenance Domain Level	Specifies the Maintenance Domain Level.
MEG End Point ID	Specifies the local and peer MEG End Point ID.
Maintenance Association ID	Specifies the Maintenance Association.

e In the options list on the left side of the tab, if the Common Header type is set to Y.1711(MPLS), select CV/FFD to turn on and set the Connectivity Verification and Fast Forward Detection settings.

Setting	Description
CV/FFD	Specifies whether the Connectivity Verification is activated
Type	Specifies the type of Connectivity Verification to be employed: CV or FFD
LSP TTSI	
LSR ID (IPv6)	Specifies the sixteen-bit source ID of the LSR (IPv6 only) for the LSP Trail Source Termination Identifier
LSP ID (Tunnel ID)	Specifies the sixteen-bit source ID of the tunnel containing the LSP Trail Source Termination Identifier data.
Expected LSP TTSI	Same as above, for received signal
Frequency	Specifies the transmission frequency of the FFD packet (FFD only).

f In the options list on the left side of the tab, if the Common Header type is set to Y.1711(MPLS), select BDI and /or FDI to turn on and set the Backward Defect Indication and/or Forward Defect Indication settings. The settings are identical for either BDI or FDI.

Setting	Description
BDI	Specifies whether the Backward Defect Indication is activated

Setting	Description
LSP TTSI	
LSR ID (IPv6)	Specifies the sixteen-bit source ID of the LSR (IPv6 only) for the LSP Trail Source Termination Identifier
LSP ID (Tunnel ID)	Specifies the sixteen-bit source ID of the tunnel containing the LSP Trail Source Termination Identifier data.
Defect Type	Specifies the type of defect indicated by the BDI or FDI.
Defect Location	Specifies the 16-bit autonomous system number for the defect location.

Step6 Press **Results** to return to the Main screen.

Step7 Connect the module to the circuit.

Step8 If you are testing an optical interface, select the **Laser** button.

Step9 Verify that the green Signal Present and Link Active LEDs are illuminated.

Step10 Select **Start Traffic** to transmit traffic over the circuit.

Step11 Use the **OAM** action buttons to manually insert an AIS, RDI, or LBM (AIS when AIS is enabled, RDI when CCM is enabled, or LBM when LBM is enabled).

Step12 Observe the Ethernet Service OAM results.

You have analyzed MPLS-TP traffic.

NOTE:

If capturing and analyzing MPLS-TP data using Wireshark, please note the following:

– If the transmitting unit's destination MAC address contains a 6 in the first four bits, Wireshark will interpret this as the fixed version field at the start of an IPv6 packet and decode it as such.

– Wireshark does not support decoding of T-MPLS OAM PDUs and will decode OAM PDUs according to ITU-T Y.1711 when it encounters label 13 (OAL), which will show erroneous fields.

Using J-Proof to verify layer 2 transparency

You can use the instrument to verify that an Ethernet circuit can support a variety of control protocols (such as CDP, VTP, STP, and RSTP), irrespective of the underlying transport method.

NOTE:

It is not possible to run OWD at the same time as a J-Proof test.

If the Test Mode is set to J-Proof for your application, you must actively transmit the test frames by pressing the **Start Frame Sequence** action button. Your unit will not automatically transmit test frames in this mode, even if automatic traffic generation is enabled.

NOTE:

Legacy JDSU test instruments identify the J-Proof applications as Layer 2 or L2 Transparency tests throughout their user interfaces. They are compatible with the J-Proof applications.

Understanding transparent loopbacks

When a JDSU Ethernet test instrument sends a *standard loopup message*, the receiving test instrument only loops back unicast test frames that satisfy its filter criteria. Pause frames, control frames, and broadcast or multicast frames *are not looped back*.

When you verify layer 2 transparency, you need the receiving test instrument to loopback all test frames, including *control frames and frames carrying a broadcast or multicast address*. To do so, you must place the traffic originating instrument into *J-Proof (transparency) mode*, and then specify the settings for the outgoing loop-up frame. When the receiving instrument receives the transparent loop-up frame, it is automatically placed into transparent loopback mode, and it returns all received test frames. *You do not need to specify filter settings on the receiving instrument.*

When initiating a transparent loopback from the traffic originating instrument, you can send the loop-up frame to a specific test instrument (by specifying the appropriate unicast destination address), or you can send a broadcast loopup frame to loop-up the first test instrument that replies within the broadcast boundary.

When the test is completed, the far end instrument is automatically taken out of loop up mode.

Configuring the traffic originating instrument

Before verifying layer 2 transparency, you must place the traffic originating instrument into *J-Proof* mode, specify the settings for the outgoing loop-up frame, and configure the outgoing control frames.

To configure the traffic originating instrument

Step1 If you haven't already done so, use the Test Menu to select the Layer 2 Traffic test application for the interface you are testing. Refer to Table 2 on page 26 for a list of layer 2 applications.

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see "Specifying interface settings" on page 46).

Step3 Select the **Ethernet** tab, and then do the following:

- **a** In Test Mode, select **J-Proof**.
- **b** Specify the remaining settings that define the characteristics of the transmitted loop back frame (see "Specifying Ethernet frame settings" on page 49). If you are looping up a specific test instrument, be certain to specify a unicast destination address for the frame.

Bear in mind that the encapsulation settings for *outgoing control frames* (as opposed to the loop-up frame) are specified on the J-Proof tab for each type of control frame.

Step4 Select the **J-Proof** tab. By default, a single test frame appears in the frame list. You can specify a name for the frame, the control protocol format, encapsulation settings, the number of frames of this type to transmit (the count), the frame rate, and the timeout period.

To modify the settings for the transmitted frame:

- **a** If you want to name the frame, select the **Test Frame** setting to launch a keypad, and then type a name using up to twenty characters. Select **OK** to close the keypad.
- **b** In **Protocol**, select the control protocol format for the frame.
- **c** In **Encap.**, select **None**, **VLAN**, or **Q-in-Q**. If you select VLAN or Q-in-Q, be certain to do the following:

VLAN. Select the **VLAN** field on the image of the outgoing frame at the bottom of the tab, and then specify the **VLAN ID** and **User Priority** for the frame. If you want the PBit to increment for each transmitted frame, select **PBit Increment**. For details on VLAN settings, refer to "Configuring VLAN tagged traffic" on page 54.

Q-in-Q. Select the **SVLAN** field on the image of the outgoing frame at the bottom of the tab, and then specify the service provider's **SVLAN ID**, **SVLAN User Priority**, **DEI Bit**, and **SVLAN TPID** for the frame. If you want the PBit to increment for each transmitted frame, select **PBit Increment**.

Select the **CVLAN** field, and then specify the customer **VLAN ID** and **User Priority** for the frame. If you want the PBit to increment for each transmitted frame, select **PBit Increment**. For details on Q-in-Q settings, refer to "Configuring Q-in-Q traffic" on page 55.

d In **Count**, specify the number of frames you want to transmit.

e In **Rate (fr/sec)**, enter the rate at which you want to transmit the frames.

f In **Timeout (msec)**, enter the number of milliseconds the instrument will wait to receive the looped back frame before stopping transmission of frames.

Step5 If you want to transmit control frames for different protocols, do the following for each protocol:

a Select the **Add Frame** soft key.

b Specify the settings listed in step 4 for each type of frame, or use the **Quick Config** soft key populate the frame list with all types of control frames, or frame types for a particular protocol family. You can also assign common encapsulation settings to all of the frame types that appear in the list using the **Quick Config** soft key (see "Using Quick Config to configure test frames" on page 76).

Step6 Press **Results** to return to the Main screen.

The traffic originating instrument is configured for a layer 2 transparency test.

Using Quick Config to configure test frames

You can quickly populate the Frames List with frame types for all available protocols, or a particular family of protocols. When you do so, all current frame settings will be overwritten, and the frame types generated by the instrument will all share the *same encapsulation settings*.

After populating the list using the Quick Config soft key, you can then optionally edit the settings for the generated frame types. For example, you can assign different VLAN priorities to the frame types.

To quickly generate and configure test frames

Step1 If you haven't already done so, use the Test Menu to select the Layer 2 Traffic test application for the interface you are testing. Refer to Table 2 on page 26 for a list of layer 2 applications.

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see "Specifying interface settings" on page 46).

Step3 Select the **Ethernet** tab, and then do the following:

a In Test Mode, select **J-Proof**.

b Specify the settings for the outgoing loop-up frame (see step 3 on page 75 of "Configuring the traffic originating instrument").

Step4 Select the **J-Proof** tab, and then select the **Quick Config** soft key.

The Quick Config dialog box appears.

Step5 Specify the following settings:

Setting	Value
Intensity	Select one of the following: – **Full.** Select full to transmit 100 frames per protocol. – **Quick.** Select Quick to transmit 10 frames per protocol.
Family	Select one of the following: – **All.** Select All to transmit frames for every supported protocol. – **Spanning Tree.** Select Spanning to transmit STP, RSTP, and MSTP frames. – **Cisco.** Select Cisco to transmit CDP, VTP, PagP, UDLD, DTP, PVST-PVST+, ISL, and STP-ULFAST frames. – **IEEE.** Select IEEE to transmit GMRP, GVRP, LACP, VLAN-BRDGSTP, and 802.1d frames.
Encapsulation	Select one of the following, and then specify the associated VLAN and, if applicable, SVLAN settings: – **None.** Select None if you do not want to transmit encapsulated frames. – **VLAN.** Select VLAN to transmit VLAN-tagged frames, then specify the associated settings. For details, refer to step c on page 75. – **Q-in-Q.** Select Q-in-Q to transmit Q-in-Q encapsulated frames, and then specify the associated customer and service provider settings. For details, refer to step c on page 75.

Step6 Select **OK** to store the settings and populate the Frames List.

Step7 *Optional.* If you would like to change settings for one or more of the frame types, do so.

The frame types are generated.

Verifying the far end filter settings

After you configure the traffic originating instrument, verify that the Encapsulation setting for the Ethernet filter is set to **Don't Care**. This ensures that traffic will be looped back.

Initiating the transparent loopback

After you configure the traffic originating instrument, and check the far end instrument's filter settings, you can initiate the transparent loopback.

To initiate the transparent loopback

Step1 If you are verifying transparency on an optical circuit, turn the Laser ON.

Step2 On the Main screen, select the **Actions** action panel, then select **Loop Up**. The instrument sends the loop-up frame.

When the receiving instrument is placed in J-Proof transparent loopback mode, a message appears stating that the remote transparent loop up was successful. You are ready to transmit the test frames.

Starting the frame sequence

After turning the laser ON (if you are testing on an optical circuit), and placing the second test instrument into transparent loopback mode, you can transmit the test frames. The frames are transmitted sequentially in the sequence used on the Frames List.

To transmit test frames

– On the Main screen, if you haven't already done so, select the **Actions** action panel, then select **Start Frame Sequence**. The instrument transmits the frames sequentially as they appear in the Frames List.

The test frames are transmitted.

Observing transparency results

After transmitting and looping back test frames, you can observe results associated with transparency testing in the J-Proof category.

To observe transparency results

– On the Main screen, set the result group to Ethernet, and the result category to J-Proof. Counts of transmitted and received frames, and the pass/fail status appears for each protocol.

Transparency results are displayed. For detailed result descriptions, refer to "J-Proof (transparency) results" on page 366.



NOTE:

When your instrument is in Transparent test mode, Payload Analysis is automatically turned OFF. If you return to Traffic mode, Payload Analysis is turned back ON.

Layer 3 testing

Using the instrument, you can transmit, monitor, and analyze layer 3 IPv4 or IPv6 traffic. Step-by-step instructions are provided in this section for the following:

– "Specifying L3 interface settings" on page 79
– "Configuring MPLS traffic" on page 80
– "Specifying transmitted IPv4 packet settings" on page 83
– "Specifying IPv4 filter settings" on page 85
– "Specifying transmitted IPv6 packet settings" on page 86
– "Specifying IPv6 filter settings" on page 87
– "Transmitting and analyzing IP traffic" on page 88
– "Ping testing" on page 89
– "Running Traceroute" on page 91
– "Monitoring IP traffic" on page 92



NOTE: IPv4 applications

You *must* select an IPv4 application if you intend to do the following:

– Establish PPPoE sessions
– Transmit and analyze MPLS encapsulated traffic on electrical or optical circuits.

NOTE: IPv6 applications

You can only run a single IPv6 application at a time. You can run other applications from other test ports (for example, a layer 2 Ethernet or layer 3 IPv4 application) while running one IPv6 application.

Specifying L3 interface settings

Before you transmit traffic, you can specify interface settings. Specification of the interface settings is similar for LAyer 2, 3 and 4 applications. Explanation of these settings can be found at "Specifying interface settings" on page 46.

Specifying the data mode and link initialization settings

Before transmitting layer 3 traffic, you must specify whether you are transmitting IPoE or PPPoE traffic (if you are testing on an electrical, 1 GigE optical, or 100 Mbps optical circuit), and provide the appropriate link initialization settings.

To specify the data mode and initialization settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the **Ethernet** tab.

Step3 In Encapsulation, select one of the following:

- **None**. If you do not want to encapsulate transmitted traffic, select **None**.
- **VLAN.** If you want to transmit VLAN tagged frames, select VLAN, and then refer to "Configuring VLAN tagged traffic" on page 54.
- **Q-in-Q.** If you want to transmit VLAN stacked (Q-in-Q) frames, select **Q-in-Q**, and then refer to "Configuring Q-in-Q traffic" on page 55.
- **MPLS.** If you are testing on an MPLS network, and you want to transmit traffic with a MPLS header, select **MPLS**, and then refer to "Configuring MPLS traffic" on page 80.

NOTE: If you selected a Terminate application, and you want to filter received traffic using MPLS criteria, *you must select MPLS encapsulation for transmitted traffic*.

Step4 In Data Mode, specify **IPoE** or **PPoE**.

Step5 If you want the unit to issue an ARP request to determine the destination MAC address of the instrument's link partner, in ARP mode, select **Enabled**; otherwise, select **Disabled**, and then be certain to manually specify the destination MAC address, (see "Specifying Ethernet frame settings" on page 49).

If you enabled ARP, and you only want to respond to ARP requests from devices on the same VLAN specified for transmitted traffic, select **Match VLAN ID(s)**.

NOTE: If you need your unit to respond to ARP requests from other devices (for example, a second test instrument on the circuit), be certain to enable ARP.

Step6 In Frame Type, specify **DIX** or **802.3**.

Step7 In Length Type, indicate whether you want to specify the length as a frame size or as a packet length.

- **Frame Size.** If you select Frame Size, select a pre-defined size, or select User Defined or Jumbo, and then specify the size. The calculated packet length (in bytes) appears to the right of the field.
- **Packet Length.** If you select Packet Length, select a pre-defined length, or select User Defined, Jumbo or EMIX and then specify the length. The calculated frame size (in bytes) appears to the right of the field.

  If you selected Random or EMIX, use the **Configure** button to specify user-defined random frame sizes, including Jumbo, or select Reset to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations. EMIX also adds the EMIX Cycle Length field that controls how many frame entries are sent, in order, before cycling back to the first frame entry and repeating. To define the number of frame entries, enter a number between 1 and 8.

Step8 If you want to specify a source address for the traffic, select **SA**, and then specify the following:

- **Source MAC Address.** Select Factory Default or User Defined.
- **User MAC Address.** If you specified User Defined, enter the source MAC address using a 6 byte hexadecimal format.

Step9 Select the **Filter** tab, and then specify the Ethernet filter settings for the destination type, source type, and encapsulation.

Configuring MPLS traffic

To configure MPLS traffic

Step1 After selecting **MPLS** as your encapsulation, do the following:

a In EtherType, select **MPLS Unicast** or **MPLS Multicast**.

b Under Configure outgoing frames, select **MPLS1 Label**, and then specify the label the network will use to route the traffic, the Priority, and the TTL value.

NOTE: MPLS settings are only available when configuring layer 3 test applications.

Step2 *Optional*. If you want to configure a second MPLS label for your traffic, in MPLS Label #, select **2**, and then repeat step 1 for the second label.

NOTE: When a unit is in LLB mode, it always uses the labels specified for the transmitted traffic; therefore:

- If your near-end module is in LLB mode and is configured to transmit traffic with a second MPLS label, but the module's link partner is configured to transmit traffic with a single label, the out of sequence and lost frames counts reported by the module's link partner may increment if the incoming frame rate is too high.
- If your near-end module is in LLB mode, and is configured to transmit traffic with a single MPLS label, but the module's link partner is configured to transmit traffic with more than one label, the near-end module’s receive bandwidth utilization will exceed its transmit bandwidth utilization.

Step3 Based on your settings, the unit automatically calculates and displays the frame size in the Calc. Frame Size field. Return to step – on page 52 of “Specifying Ethernet frame settings” for details on specifying the remaining settings.

MPLS settings are specified.

Specifying PPPoE settings

In addition to the settings you specify to establish an Ethernet link, when establishing a PPPoE session (available for compatible IPv4 Terminate applications only), you also specify settings that allow you to log in to the PPPoE peer. The settings indicate whether you want your unit to emulate a PPPoE client or server, and provide the user name, password, and other information required to establish the session.

To specify the PPPoE settings and establish a connection

Step1 If you haven't already done so, use the Test Menu to select an IPv4 test application in Terminate mode for the e10/100/1000 electrical interface.

Step2 Select the **Setup** soft key, and then select the **Ethernet** tab. Verify that the Data Mode is set to PPPoE.

Step3 Go to the PPP setup tab, then specify the following settings. The Provider Name, Password, and Service Name you specify for the instrument must match those of its PPPoE peer:

Settings	Parameters
PPP Mode	– Client. In most instances, the instrument should emulate a PPPoE client. If you select Client mode, you do not need to specify the Local IP, Subnet Mask, or Remote IP settings on the IP setup tab because they will be provided by a PPPoE server. – Server. Select Server mode if the unit must operate as a PPPoE server. For example, if the unit is positioned before a BBRAR (Broadband Remote Access Router), it must function as a server. If you select Server mode, you must specify the Local IP, Subnet Mask, or Remote IP settings on the IP setup tab.
User Name	Enter a valid user name for the ISP (Internet Service Provider).
Password	Enter the password for the user name that you specified. Remember passwords are often case-sensitive.
Service Provider	If the ISP requires the provider's domain name be included with the User Name (for example, joesmith@provider.net), select this setting, and then specify the provider name. An at sign (@) and the provider name will automatically be appended to the User Name that you specified, and will be carried in the packet.
Service Name	Select this setting if you want to specify a service name. If you specify a service name, your unit will only attempt to establish a PPPoE session with the service you specify. The default service name is "JDSU".

Step4 Do one of the following:

– If the instrument is emulating a PPPoE client, proceed to step 5. The unit will use a static IP address.

– If the instrument is emulating a PPPoE server, go to the IP setup tab, and then specify the following settings:

Settings	Parameters
Local IP	Enter the source IP address for traffic generated by your unit. This address is used as the remote IP address for the PPPoE client.
Subnet Mask	Enter the subnet mask.

Settings	Parameters
Remote IP	Enter remote IP address for the instrument server. This address is used as the local (source) IP address on the client side of the connection.

NOTE:
The instrument's PPPoE server is a demo server and does not support full server functionality.

Step5 If you need to specify other settings for the test, do so; otherwise, return to the Main screen and do the following:

a Press the **PPPoE Client Log-On** or **PPPoE Server Log-On** Action key.

The unit discovers the MAC address of the PPPoE peer, and then uses the MAC address in combination with a session ID to uniquely identify the session.

b Observe the messages and events associated with the PPPoE login process. For a list of potential messages, see "PPPoE messages" on page 82.

The PPPoE session is established. The instrument will continuously send PPP echoes and replies to keep the session established.

PPPoE messages

The following messages may appear in the during the PPPoE login process.

Table 9 PPPoE messages

Message	Typically Indicates:	Resolution
PPP Authentication Failed	The user name, password, or provider name you specified were not accepted by the PPPoE server.	– It is possible that the user name and password you specified were not recognized by the PPPoE server. Verify that you specified the correct name and password. – If the PPPoE server requires a provider name, verify that the name you specified when you configured the PPP settings is correct. – It is possible that the PPPoE server does not require a provider name; if so, specifying one in the PPP settings results in a failed authentication. Set the Provider Name setting to **No**, and then try to establish the session again. – Try to establish a new session with the server.
PPPoE Timeout	The instrument is not physically connected to a PPPoE server, or it is configured to use a service that is not supported by the server.	– Verify that the instrument is physically connected to the server. – Verify that the service name you specified is correct, or, if a service name is not required by the server, set the Service Name setting to **No**. – Try to establish a new session with the server.

Table 9 PPPoE messages (Continued)

Message	Typically Indicates:	Resolution
Data Layer Stopped	The physical Ethernet link to the instrument is lost.	Reconnect the physical Ethernet link. The instrument will attempt to reconnect to the server.
PPP LCP Failed	There is a problem with the server.	Try to establish a new session with the server.
PPP IPCP Failed		
PPPoE Failed		
PPP Up Failed	The PPPoE server dropped a successful PPPoE session.	Try to establish a new session with the server.
Internal Error - Restart PPPoE	The instrument experienced an internal error.	Try to establish a new session with the server.

Terminating a PPPoE session

After testing is complete, you must manually terminate the PPPoE session.

To terminate a PPPoE session

– Press the **PPPoE Client Log-Off** or **PPPoE Server Log-Off** Action key.

Specifying transmitted IPv4 packet settings

Before you transmit layer 3 IPv4 traffic, you can specify the IP characteristics of the traffic, such as the destination IP address, the type of payload, and the type of service.

To specify transmitted IPv4 packet settings

Step1 If you haven't already done so, use the Test Menu to select the layer 3 or layer 4 IPv4 test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the **IP** tab.

Step3 In Length Type, indicate whether you want to specify the length as a frame size or as a packet length.

– **Frame Size.** If you select Frame Size, you must specify the size on the Ethernet tab, then return to the IP tab to specify the remaining settings.

– **Packet Length.** If you select Packet Length, select a pre-defined length, or select User Defined or Jumbo and then specify the length. The calculated frame size (in bytes) appears to the right of the field.

  If you selected Random or EMIX, use the **Configure** button to specify user-defined random frame sizes, including Jumbo, or select Reset to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations. EMIX also adds the EMIX

Cycle Length field that controls how many frame entries are sent, in order, before cycling back to the first frame entry and repeating. To define the number of frame entries, enter a number between 1 and 8.

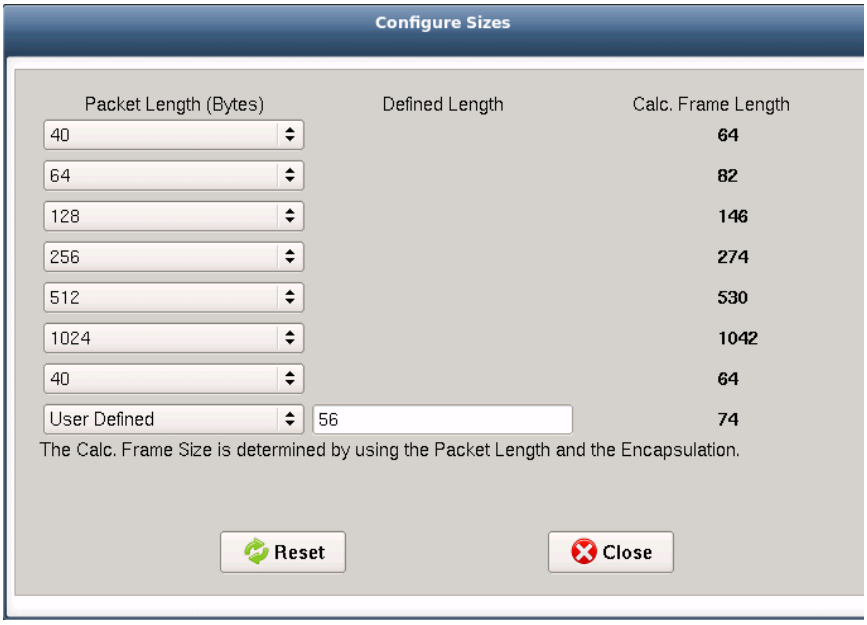


Figure 18 Configure Frame Size

Step4 On the illustration of the IP packet, select the **TOS/DSCP** field, and then do the following to indicate how the packet should be prioritized during the transmission:

– In Type, select **TOS** or **DSCP**.

– Specify the TOS or DSCP value. DSCP values are shown as code points with their decimal values in ( ) following. For example: EF(46).

Step5 Select the **TTL** field, and then specify maximum number of hops to travel before the packet is dropped.

Step6 Select the **Source/Destination Address** field, and then specify the Source IP Type, Source IP, Default Gateway, Subnet Mask and Destination IP. For load balanced situations a fixed IPv4 length may cause problems. ID incrementing can eliminate this problem. To enable ID incrementing, set the IP ID Increment field to Enable.

Step7 To verify the validity of the Destination IP entered, select the Ping button. If a connection to the specified IP address is possible, a green check mark will display after the Destination IP field. If no connection is possible a red “X” will appear. This ping result will also appear on the ping button on the Results page.

NOTE:

For optical applications the Laser must be ON to ping the destination IP.

Step8 Select the Data field, and then do the following:

– If you want to transmit packets with a time stamp and sequence number, select **Acterna**.

Indicate whether you want the payload to carry a BERT pattern, or a Fill-Byte pattern, then specify the pattern.



NOTE:

In 10M/100M/1GbE/10G, 40Gig,and 100Gig Traffic applications, you can also select either Version 2 or Version 3 Acterna Payload (ATP). To successfully use the Version 3 payload, the remote equipment must be capable of receiving Version 3 payloads. Verify compatibility before selecting Version 3 payloads.

– If you are measuring round trip delay on a 10 Gigabit circuit, in RTD Setup, indicate whether you want to measure delay with a high degree of precision, or a low degree of precision. In most instances, you should select **High Precision - Low Delay**.

  NOTE: You must select an Acterna payload to measure round trip delay and count lost packets.

– If you want to populate the payload by repeating a specific pattern of bytes, select **Fill Byte**, type the byte value using a 1 byte hexadecimal format, and then specify the **Protocol**.

Step9 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The transmitted IPv4 packet settings are specified.

Specifying IPv4 filter settings

Before transmitting layer 3 IPv4 traffic, you can optionally specify settings that indicate the expected received payload and determine which packets will pass through the receive filter and be counted in the test result categories for filtered IP traffic. The settings may also impact other results.

To specify received IPv4 packet settings

Step1 If you haven't already done so, use the Test Menu to select the IPv4 test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for lists of layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the **Filters** tab.

Step3 In the panel on the left side of the tab, select **Basic**, then set the Filter Mode to **Detailed**.

Step4 Specify the Ethernet filter settings (see "Specifying Ethernet filter settings" on page 56.

Step5 To specify layer 3 filter settings, in the panel on the left side of the tab, select **IP**.

Step6 Set the IP Filter to **Enable**., then do the following:

a If you are running an application in Monitor mode, in **IP Version**, select IPv4.

b In **Address Filter**, select one of the following:

Single Direction. To pass through the filter, traffic must satisfy the source and destination address criteria you specified for the filter to be reflected in the L3 Filter Counts and L3 Filter Stats result categories.

Either Direction. The filter will not care which direction the traffic is coming from; therefore, the source address carried in the filtered traffic can be the source address of the near-end unit or port, or the source address of the far end unit or port. Traffic from either source will be reflected in the L3 Filter Counts and L3 Filter Stats result categories.

c On the illustration of the IP packet, select the **TOS/DSCP**, **Protocol**, **Source IP**, or **Destination IP** field, and then enter the filter criteria. This is the criteria that must be carried in the analyzed (filtered) traffic. For descriptions of each of these settings, see "Specifying transmitted IPv4 packet settings" on page 83.

Step7 If you want the module to monitor and analyze live Ethernet traffic, in the panel on the left side of the tab, select **Rx Payload**, then turn Payload Analysis Off. The instrument will suppress lost frames (LF) in their associated result counts and as triggers for LEDs.

Step8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The filter settings for IPv4 packets are specified.

Specifying transmitted IPv6 packet settings

Before you transmit layer 3 IPv6 traffic, you can specify the IP characteristics of the traffic, such as the source type and default gateway.

To specify transmitted IPv6 packet settings

Step1 If you haven't already done so, use the Test Menu to select the layer 3 or layer 4 IPv6 test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the **IP** tab.

Step3 In Length Type, indicate whether you want to specify the length as a frame size or as a packet length.

- **Frame Size.** If you select Frame Size, you must specify the size on the Ethernet tab, then return to the IP tab to specify the remaining settings.
- **Packet Length.** If you select Packet Length, select a pre-defined length, or select User Defined, Jumbo, or Random and then specify the length. The calculated frame size (in bytes) appears to the right of the field.

  If you selected Random or EMIX, use the **Configure** button to specify user-defined random frame sizes, including Jumbo, or select Reset to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations. EMIX also adds the EMIX Cycle Length field that controls how many frame entries are sent, in order, before cycling back to the first frame entry and repeating. To define the number of frame entries, enter a number between 1 and 8.

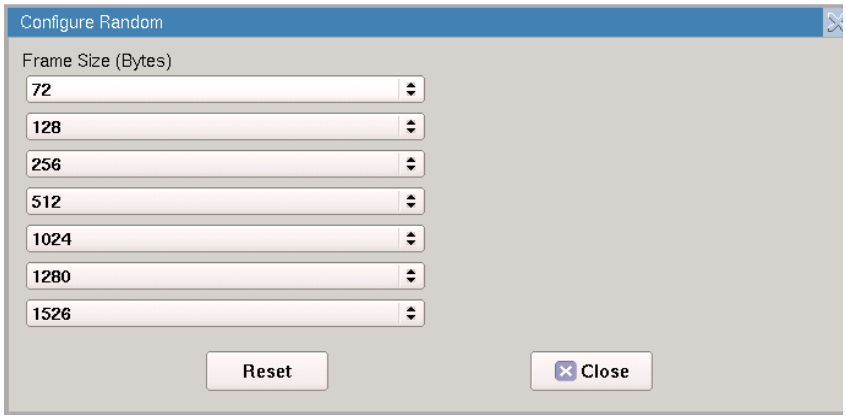


Figure 19 Configure Random Frame Size

Step4 On the illustration of the IP packet, select the **Traffic Class** field, and then specify a number representing the traffic class using a hexadecimal format ranging from 0x0 to 0xFF.

Step5 Select the **Flow Label** field. If you are certain the routers on the circuit support flow labels for traffic prioritization, specify the flow label using a hexidecimal format ranging from 0x0 to 0xFFFFF; otherwise, use the default (0x0).

Step6 Select the **Next Header** field, then specify the code representing the type of data carried in the next header in the packet using a hexidecimal format ranging from 0x0 to 0xFF.

Step7 Select the **Hop Limit** field, then specify the time after which a packet can be deleted by any device on a circuit as a number of hops. The default Hop Limit setting is 64 hops.

Step8 Select the **Source Address** field, then select one of the following:

- **Stateful.** Select Stateful if you want to obtain the required global, default gateway, and DNS server addresses from a DHCPv6 server.
- **Stateless.** Select Stateless if you know that routers on the network allow stateless configuration. When you use Stateless configuration, the instrument generates a tentative link-local address, and then performs Duplicate Address Detection to verify that the address isn't already used. If DAD is successful, the instrument then obtains a subnet prefix from the router to build the required global address.
- **Manual.** Select Manual if you want to specify the source link-local address, global address, subnet prefix length, and default gateway.

Step9 Select the **Destination Address** field, and then specify the destination address for the traffic.

Step10 Select the Data field, and then select do the following:

- If you want to transmit packets with a time stamp and sequence number, select **Acterna**.

  Indicate whether you want the payload to carry a BERT pattern, or a Fill-Byte pattern, then specify the pattern.
- If you are measuring round trip delay on a 10 Gigabit circuit, in RTD Setup, indicate whether you want to measure delay with a high degree of precision, or a low degree of precision. In most instances, you should select **High Precision - Low Delay**.

  NOTE: You must select an Acterna payload to measure round trip delay and count lost packets.
- If you want to populate the payload by repeating a specific pattern of bytes, select **Fill Byte**, type the byte value using a 1 byte hexadecimal format, and then specify the **Protocol**.

Step11 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The transmitted IPv6 packet settings are specified.

Specifying IPv6 filter settings

Before transmitting layer 3 IPv6 traffic, you can optionally specify settings that indicate the expected received payload and determine which packets will pass through the receive filter and be counted in the test result categories for filtered IPv6 traffic. The settings may also impact other results.

To specify received IPv6 packet settings

Step1 If you haven't already done so, use the Test Menu to select the IPv6 test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for lists of layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Select the **Setup** soft key, and then select the **Filters** tab.

Step3 In the panel on the left side of the tab, select **Basic**, then set the Filter Mode to **Detailed**.

Step4 Specify the Ethernet filter settings (see “Specifying Ethernet filter settings” on page 56.

Step5 To specify layer 3 filter settings, in the panel on the left side of the tab, select **IP**.

Step6 Set the IP Filter to **Enable**, then do the following:

a If you are running an application in Monitor mode, in **IP Version**, select IPv6.

b In **Address Filter**, select one of the following:

Single Direction. To pass through the filter, traffic must satisfy the source and destination address criteria you specified for the filter to be reflected in the L3 Filter Counts and L3 Filter Stats result categories.

Either Direction. The filter will not care which direction the traffic is coming from; therefore, the source address carried in the filtered traffic can be the source address of the near-end unit or port, or the source address of the far end unit or port. Traffic from either source will be reflected in the L3 Filter Counts and L3 Filter Stats result categories.

c On the illustration of the IP packet, select the **Traffic Class**, **Next Header**, **Source Address**, or **Destination Address** field, and then enter the filter criteria. This is the criteria that must be carried in the analyzed (filtered) traffic. For descriptions of each of these settings, see “Specifying transmitted IPv6 packet settings” on page 86

Step7 If you want the module to monitor and analyze live Ethernet traffic, in the panel on the left side of the tab, select **Rx Payload**, then turn Payload Analysis Off. The instrument will suppress lost frames (LF) in their associated result counts and as triggers for LEDs.

Step8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The filter settings for IPv6 packets are specified.

Transmitting and analyzing IP traffic

Before you transmit layer 3 IP traffic, you must specify:

– Interface settings (see “Specifying interface settings” on page 46).
– IP characteristics of the transmitted traffic (see “Specifying transmitted IPv4 packet settings” on page 83).
– IP characteristics used to filter received traffic (see “Specifying IPv4 filter settings” on page 85).
– Traffic load settings (see “Specifying traffic load settings” on page 64).

After you configure the layer 3 IP settings, and you either manually specify the destination device’s MAC address, or the unit determines the address using ARP, you are ready to transmit traffic over the link.

To transmit and analyze IP traffic

Step1 Use the Test Menu to select the layer 3 IP traffic terminate test application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see “Specifying interface settings” on page 46).

Step3 Specify settings that define the Ethernet frame and the IP packet characteristics of the transmitted traffic (see “Specifying transmitted IPv4 packet settings” on page 83).

Step4 Select the **Setup** soft key, and then select the **Ethernet filter** tab to specify the Ethernet filter settings (see “Specifying Ethernet filter settings” on page 56.

Step5 Select the **IP Filter** tab to specify settings that filter the received traffic based on specified packet characteristics (see “Specifying IPv4 filter settings” on page 85).

Step6 Select the **Traffic** tab to specify the type of load the unit will transmit (see “Specifying traffic load settings” on page 64).

Step7 Press **Results** to return to the Main screen.

Step8 Connect the module to the circuit.

Step9 If you are testing an optical interface, select the **Laser** button.

Step10 Select **Start Traffic** (for constant or bursty loads) or **Start Ramp** (for ramped loads) to transmit traffic over the circuit.

Step11 Verify that the green Signal Present, Sync Acquired, Link Active, and IP Packet Detect LEDs are illuminated.

Step12 At a minimum, observe the summary, layer 2 and 3 link counts and statistics, layer 2 and 3 filter counts and statistics, layer 3 configuration status, and error statistics.

You have analyzed IP traffic.

Ping testing

Using the instrument, you can verify connectivity with another layer 3 or IP device by sending ping request packets to the device. The device then responds to the ping request with a ping reply (if the device is responsive), or with another message indicating the reason no ping reply was sent.

Ping testing tells you if the destination device is reachable, how long it took the ping packet to travel to the destination device and back to the Transport Module, and if ping packets were dropped or lost along the way.



NOTE:

Ping application testing differs from ping testing during setup in that the ping applications are not able to respond to mismatched frames. Ping testing during setup is a simple IP address connectability verification.

Before you transmit ping request packets, you must specify:

– Interface settings (see “Specifying interface settings” on page 46).

– Ethernet Frame settings (see “Specifying Ethernet frame settings” on page 49. Bear in mind that Jumbo packets are only supported for DIX traffic (the 802.3 specification does not support jumbo packets).

  Jumbo frames are also not supported when the instrument is configure to transmit fast ping packets.

– IP settings (see “Specifying IP settings for Ping and Traceroute testing” on page 90).

After you specify the ping settings, you are ready to transmit ping request packets.



NOTE:

If you are transmitting ping packets larger than 2000 bytes to an MTS 8000 Transport Module, the Transport Module will not respond. This is not an issue when testing using two MSAMs, or one MSAM and an FST-2802.

Specifying IP settings for Ping and Traceroute testing

Before you transmit ping request packets or run the Traceroute application, you can specify settings indicating the source of the IP address (static, or assigned by a DHCP server), and the destination type (IP address or host name), and attributes of the ping request packets (type, size, type of service, and time to live). ARP is always enabled when running Ping and Traceroute applications.

To specify IP settings

Step1 If you haven't already done so, use the Test Menu to select the Ping application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Select the **Setup** soft key, select the **Ethernet** tab, and then specify the Ethernet frame settings (see "Specifying Ethernet frame settings" on page 49). Be certain to set the data mode (IPoE or PPPoE).

Step3 Select the **IP** tab.

Step4 In Source Type, select one of the following:

- **Static IP**. To manually assign an IP address as the source address for the traffic, select **Static IP**, and then type the address, subnet mask, and default gateway in the corresponding fields.
- **DHCP**. To allow a DHCP server to assign an IP address, subnet mask, and default gateway, select **DHCP**.

Step5 In Destination Type, select IP Address or Host Name, and then type the destination IP address or the host name for the ping.

Step6 If you selected the Ping application, under Ping, specify the following settings:

a In Ping Type, indicate whether you want to transmit a **Single** ping packet, **Multiple** ping packets, a **Continuous** stream of ping packets, or a **Fast** stream of ping packets. If you specify Multiple, enter the number of packets to transmit.

NOTE: The instrument sends multiple and continuous pings at a rate of 1 ping per second.

It sends fast pings at a rate of once every 100 ms; assuming a response is received within 100 ms. If the unit doesn't receive a reply within 100 ms, it will wait up to one additional second for a reply. If a reply is received, it will then send another ping packet. Therefore, this setting may result in very fast ping transmissions, or slower transmissions, depending on the responsiveness of the network.

b In Packet Size (Bytes), enter the size of the ping request packet or packets.

c In TOS Type, specify **Type of Service** or **DSCP**, and then enter the type of service code (see "Specifying transmitted IPv4 packet settings" on page 83).

d In Time To Live, specify the number of hops the packet can travel before being dropped.

NOTE: The default TTL for ping packets is 64.

Step7 If you selected the Traceroute application, under Traceroute, specify the following settings:

a In TOS Type, specify **Type of Service** or **DSCP**, and then enter the type of service code *(see "Specifying transmitted IPv4 packet settings" on page 83).

b In Max Num. Hops (TTL), enter the number of hops or TTL after which the TTL value stops increasing.

c In Response Time (s), enter the number of seconds the module will wait for a response from a hop.

Step8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The IP settings for ping testing are specified.

Transmitting ping request packets

After you specify interface, frame, and IP settings, you can transmit ping request packets to verify connectivity.

To transmit ping packets

Step1 Use the Test Menu to select the layer 3 Ping test application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see "Specifying interface settings" on page 46).

Step3 Select the **Ethernet Frame** tab to specify settings that define the frame characteristics of the transmitted traffic, and then select the **IP** tab to specify settings that characterize the ping packets (see "Specifying IP settings for Ping and Traceroute testing" on page 90).

Step4 Press **Results** to return to the Main screen.

Step5 Connect the module to the circuit.

Step6 If you are testing an optical interface, select the **Laser** button.

Step7 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step8 On the Main screen, select the **Ping** button to transmit the packet or packets.

Step9 At a minimum, observe the ping and IP configuration status test results.

You have transmitted ping request packets.

Running Traceroute

Before you run the traceroute application to determine where problems in the network are occurring, you specify the interface settings, frame characteristics of the traffic, and settings that control the traceroute application, such as the source and destination IP addresses, maximum number of hops, and the response time.

To run traceroute

Step1 Use the Test Menu to select the Traceroute application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see "Specifying interface settings" on page 46).

Step3 Select the **Setup** soft key, select the **Ethernet** tab, and then specify the Ethernet frame settings (see "Specifying Ethernet frame settings" on page 49). Be certain to set the data mode (IPoE or PPPoE).

Step4 Select the **IP** tab, and then specify the IP settings for the traceroute (see "Specifying IP settings for Ping and Traceroute testing" on page 90).

Step5 Press **Results** to return to the Main screen.

Step6 Connect the module to the circuit.

Step7 If you are testing an optical interface, select the **Laser** button.

Step8 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step9 Using the View menu, set the result display to a full view (Full Size), and then select the Traceroute result category.

Step10 Press the **Traceroute** action button.

Step11 Observe the traceroute.

The traceroute application is finished.

Monitoring IP traffic

You can use the instrument to monitor IP traffic when you test each of the Ethernet interfaces. Before you monitor traffic, you can specify interface settings and settings that characterize and filter the received IP traffic.



NOTE:

If you are analyzing traffic on an optical circuit, be certain to turn the laser on.

To monitor IP traffic

Step1 Use the Test Menu to select the layer 3 monitor/through application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see “Specifying interface settings” on page 46).

Step3 Do one of the following:

- If you want to filter the received packets based on their Ethernet frame settings, select the **Ethernet Filter** tab, and then proceed to step 4 and step 5; otherwise, proceed to step 8.
- If you want to filter received MPLS packets based on the MPLS packet settings, select the Ethernet Filter tab, set encapsulation to MPLS, and then specify the filter criteria (see “Filtering traffic using MPLS criteria” on page 61).

Step4 Under **Configure incoming frames**, do the following:

- In **Destination Type**, specify the destination address type corresponding to the Destination Address in the received frames.
- In **Source Type**, specify the source address type corresponding to the Source Address in the received frames.
- If you specified a Unicast or Multicast Source or Destination Type, enter the corresponding MAC address in the field provided.

Step5 In Encapsulation, do the following:

- If you want to monitor VLAN, Q-in-Q, or MPLS encapsulated traffic, select the encapsulation, and then specify the corresponding filter settings.
- If you want to monitor traffic with no encapsulation, select **None**.
- If you don’t care whether they are tagged, select **Don’t Care**.

Step6 If you want to filter the received packets based on their source IP address, destination IP address, type of service, or IP version, select the IP Filter tab, and then proceed to step 7; otherwise, proceed to step 8.

Step7 In IP Filter, select **Enable**, and then specify the following filter criteria:

- To filter traffic for a specific source IP address, select **Yes**, and then type the source address.
- To filter traffic for a specific destination IP address, select **Yes**, and then type the destination address.
- Specify whether you want to filter traffic in a single direction, or in either direction.
- To filter traffic for a specific source or destination subnet, select **Prefix Length** or **Subnet Mask**, and they type the corresponding value in the field provided.
- To filter traffic for a specific type of service or DSCP, select TOS or DSCP, and then type the corresponding value (see "Specifying transmitted IPv4 packet settings" on page 83).

Step8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

Step9 Connect the module to the circuit.

Step10 If you are testing an optical interface, select the **Laser** button.

Step11 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step12 If you selected an optical application, select **Connect Rx to Tx**. This setting does not appear for electrical applications.

Step13 At a minimum, observe the summary, layer 3 link statistics and counts, layer 3 filter statistics and counts, layer 3 configuration status, and error statistics.

Layer 3 IP traffic is monitored.

Capturing packets for analysis

If your instrument is configured and optioned to do so, you can use it to capture transmitted and received packets, save it on the instrument or to an external USB key, and then either send the packets to another technician for analysis, or analyze it yourself using the Wireshark® protocol analyzer, or the J-Mentor utility (provided on the instrument).



NOTE:

The term "packets" is used interchangeably with "frames" throughout the following section, and represents any of the layer 2, layer 3, or layer 4 datagrams carried in the traffic stream.

You can capture packets when running any of the single stream or multiple stream Ethernet, IP, TCP/UDP, or VoIP applications, with the following exceptions:

- Applications with Mac-in-Mac (MiM) encapsulated traffic
- IPTV applications

What is captured?

All received traffic (test traffic, control plane traffic, and live traffic) that satisfies the user-specified criteria on the Filter setup tab can be captured for all supported interfaces.

All transmitted traffic (test traffic, control plane traffic, and live traffic) that satisfies the user-specified criteria on the Capture setup tab can be captured for all supported interfaces up to 1 Gigabit Ethernet.

When capturing transmitted traffic from a 10 Gigabit Ethernet interface, only control plane traffic is captured.

Ethernet frames ranging from 64 to10000 bytes long can be captured, but the 4 byte Ethernet FCS is not stored in the capture buffer.

Test traffic

Test traffic is the traffic generated and transmitted by your test instrument carrying an ATP or BERT payload. Test traffic can be captured when it is transmitted, looped back and then captured when it is received, or it can be captured when received from a transmitting instrument on the far end.

You can capture received test traffic for all supported interfaces; you can capture transmitted test traffic for all supported interfaces except 10 Gigabit Ethernet.

Control plane traffic

Control plane traffic is traffic used to establish a connection with another network element (or instrument), request information from the element, or to verify connectivity with the element. Examples of control plane traffic include ARP packets, Ping packets, and software application layer datagrams, such as HTTP, TCP/UDP, or FTP control packets.

You can capture transmitted and received control traffic from all supported interfaces.

How much can be stored in the buffer?

When you configure your instrument to capture packets, you can control the size of the buffer by specifying a size ranging from 1 MB to 256 MB in 1 MB increments. You can also control how your instrument handles the packets when the buffer becomes full. The instrument can stop capturing packets entirely, or it can wrap (overwrite) the oldest packets in the buffer with new captured packets in 1 MB increments.

After capturing packets to the buffer, you can save them to a a PCAP (packet capture) file, which can optionally be compressed using gzip for efficient storage.

Why use packet slicing?

When you configure your instrument to capture packets, you can tell the instrument to capture *only the first 64 or 128 bytes of each packet*. This allows you to analyze the most important data carried in the packet headers (at the beginning of the packets), and to capture and store more packets in the buffer.

Understanding the Capture toolbar

The buttons on the Capture toolbar (illustrated in Figure 20) are used to enable or disable the capture feature, start and stop the capture process, save the packets in the capture buffer to the internal USB drive (or an external drive), or launch Wireshark® or J-Mentor to analyze the packets on the instrument.



Figure 20 Capture Toolbar

The % Buffer Full gauge shows the percentage of the available buffer capacity that is used.

When you capture traffic at a high bandwidth or specify a small buffer size, if you configure the capture to wrap (overwrite) the oldest packets in the buffer with new captured packets in 1 MB increments, the buffer gauge may appear to “jump around”. If you do not wrap the packets, the capture process may stop very soon after you start it, because the buffer reaches capacity quickly. This is expected behavior.

Specifying filter settings

If you specify filter settings when you configure the application, the settings determine which *received traffic* is captured to the buffer. The Capture Toolbar (illustrated in Figure 20) indicates whether filters are active or inactive.

Transmitted control plane frames are always captured to the buffer. When capturing frames on circuits at rates up to 1 Gigabit Ethernet, all other transmitted frames are captured.

To specify filter settings before capturing frames

Step1 If you haven’t already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 On the Main screen, select the Capture tool bar, then enable the capture feature.

Step3 Select the **Setup** soft key, and then select the **Filters** tab. By default, a summary of all currently configured filter settings appear (Ethernet, IP, and TCP/UDP).

Step4 If you would like to clear the filters (to specify new settings for the capture process), select **Clear All Filters**.

Step5 If you launched a layer 2 application, the panel on the left of the tab displays the Summary and Ethernet selections.

If you launched a layer 3 or layer 4 application, the panel displays the Summary, Basic, Ethernet, IP, and if applicable, TCP/UDP selections.

Do one of the following:

– If you launched a layer 2 application, select **Ethernet**, and then specify the settings that capture the received traffic that you want to analyze (see "Specifying Ethernet filter settings" on page 56).

– If you launched a layer 3 or layer 4 application, and you want to specify basic filter information, select **Basic**, and then specify the **Traffic Type** and the **Address Type** carried in the received traffic you want to **capture**.

– If you launched a layer 3 or layer 4 application, and you want to specify detailed filter information, select **Basic**, and then set the filter mode to **Detailed**.

  Use the Ethernet, IP, and TCP/UDP selections in the pane on the left to display the filter settings for your particular test, and then specify the settings that capture the received traffic that you want to analyze (see "Specifying Ethernet filter settings" on page 56, "Specifying IPv4 filter settings" on page 85, and "Filtering received traffic using layer 4 criteria" on page 155).

The filter settings are specified for the capture.

Capturing packets

There are two ways to capture packets

– manually starting and stopping the capture

– capturing packets based on a triggering event

Manually capturing packets

Capturing packets involves launching and configuring an Ethernet, IP, TCP/UDP, or VoIP application, specifying the capture settings, and, if you are capturing received traffic, specifying the filter settings. If you are capturing received traffic only, you can start the capture process immediately.

If you intend to capture transmitted or looped back traffic, you must actively start traffic transmission. The traffic can then be looped back (to be captured by the transmitting instrument), or captured by a second receiving instrument on the circuit.

When capturing packets in Monitor or Terminate mode, you must use Port 1 for your test if using a MSAMv1; for MSAMv2, either port can be used.

If you are capturing packets while running the VoIP application, it is recommended that you do not save the captured packets until the call is ended (the phone is on hook).

When capturing packets, bear in mind that configuring the capture for a large buffer (for example, 256 MB) with small packets (for example, 46 byte ping packets), it will take a long time to fill the buffer. If you configure the capture for a small buffer with large packets, it will take much less time.

To capture packets on the instrument

Step1 Launch a single or multiple stream layer 2 Ethernet, layer 3 IP, or layer 4 TCP/UDP application.

Step2 If you haven't already done so, on the Main screen, select the Capture tool bar, then enable the capture feature.

Step3 Select the **Setup** soft key, and then do one of the following:

– Specify the settings required to filter received traffic for the type you want to capture and analyze.

– Clear all of the filters to capture all received traffic.

For details, refer to "Specifying filter settings" on page 95.

Step4 Select the **Capture** setup tab, and then specify the following settings:

Setting	Parameter
Capture buffer size (MB)	Specify a size ranging from 1 to 256 MB in a 1 MB increment. The default buffer size is 16 MB.
Capture frame slicing	If you want to capture the first 64 or 128 bytes of each frame (and ignore the rest of the frame), select 64 or 128; otherwise, select None. If you select None (the default), the entire frame is captured.
When capture buffer is filled	If you want to overwrite the oldest packets with new packets when the buffer becomes full, select **Wrap Capture**; otherwise, select **Stop Capture**.
Include frames from Traffic tab	If you want to capture transmitted frames (the traffic load which is specified on the Traffic tab), select **Yes**.

Step5 Select the **Results** soft key to return to the Main screen.

Step6 If you are capturing transmitted or looped back traffic, select **Start traffic**.

Step7 Select the Capture toolbar, and then do the following:

a Select **Start Capture**.

A message appears in the message bar indicating that the capture has started, and the action key states **Capture Started**.

b If you want to capture packets that shows how the traffic is impacted by various events, use the buttons on the Actions, Errors, and Fault Signaling tool bars to insert the events into the transmitted traffic stream.

Step8 If you want to manually stop capturing packets (for example, after the instrument has transmitted and received a certain number of frames), select the **Capture Started** action key.

The action key turns gray, and a message appears in the message bar indicating that the capture is complete.

Packets were captured and are stored temporarily in the capture buffer. A count of the number of packets processed is provided in the Ethernet result group, in the Capture category.



WARNING: Changing applications or turning OFF the instrument

You will lose the entire contents of the capture buffer if you launch a new application on the port that you are capturing packets on, or if you turn your instrument OFF. To ensure that the packets are stored, save the capture buffer before changing applications or turning the instrument OFF.

Capturing packets based on a trigger

When troubleshooting problems that occur intermittently or inconsistently, the trigger feature allows capture to begin based on a given event. For this scenario, the filters are used as triggers.

Triggering using only the byte pattern as a trigger

Step1 Press the **Setup** soft key.

Step2 Select Capture tab, and then set **Capture** to **Enable**.

Step3 Set **Use Filters as** to **Filter**.

Step4 Select the **Filters** tab, and then, in the panel on the left side, select **Summary**.

Step5 Select the **Clear All Filters** button to clear any current filter settings.

Step6 In the panel on the left side, select **Byte Pattern**.

Step7 Set **Use Byte Pattern as** to **Trigger**, and then specify the trigger/filter as described in "Filtering traffic using byte pattern criteria" on page 62.

Step8 Select the **Capture** tab and specify a **Post-Trigger Size**. This is the amount of data, in MB, to capture after the trigger event occurs. If set to zero, the capture stops immediately after the trigger event.

Step9 Select the **Results** soft key to return to the Main screen.

NOTE:

When capturing packets based on a trigger, the capture buffer saves in wrap-around mode (over-write the oldest packets with new packets when the buffer becomes full).

Step10 Select the **Capture** toolbar, and then select **Start Capture**.

A message appears in the message bar indicating that the capture has started, and the action key states **Capture Started**.

The capture will begin when the trigger event occurs which will be when the data matches the byte pattern criteria. Captured packets are stored temporarily in the capture buffer. A count of the number of packets processed is provided in the Ethernet result group, in the Capture category.

WARNING: Changing applications or turning OFF the instrument

You will lose the entire contents of the capture buffer if you launch a new application on the port that you are capturing packets on, or if you turn your instrument OFF. To ensure that the packets are stored, save the capture buffer before changing applications or turning the instrument OFF.

Triggering using only the filters as a trigger

Step1 Press the **Setup** soft key.

Step2 Select Capture tab, and then set **Capture** to **Enable**.

Step3 Set **Use Filters as** to **Trigger**.

Step4 Select the **Filters** tab, and then, in the panel on the left side, select **Summary**.

Step5 Select the **Clear All Filters** button to clear any current filter settings.

Step6 In the panel on the left side, select **Byte Pattern**.

Step7 Set the **Use Byte Pattern as** to **Don't Care** to turn off the byte pattern as a trigger.

Step8 On the Filters tab, specify the trigger/filter as described in "Specifying filter settings" on page 95.

Step9 Select the **Capture** tab and specify a **Post-Trigger Size.** This is the amount of data, in MB, to capture after the trigger event occurs. If set to zero, the capture stops immediately after the trigger event.

NOTE:

When capturing packets based on a trigger, the capture buffer saves in wrap-around mode (overwrite the oldest packets with new packets when the buffer becomes full).

Step10 Select the **Capture** toolbar, and then select **Start Capture**.

A message appears in the message bar indicating that the capture has started, and the action key states **Capture Started**.

The capture will begin when the trigger event occurs which will be when the data matches the filter criteria. Captured packets are stored temporarily in the capture buffer. A count of the number of packets processed is provided in the Ethernet result group, in the Capture category.

WARNING: Changing applications or turning OFF the instrument

You will lose the entire contents of the capture buffer if you launch a new application on the port that you are capturing packets on, or if you turn your instrument OFF. To ensure that the packets are stored, save the capture buffer before changing applications or turning the instrument OFF.

Triggering using the filters and byte pattern simultaneously as a trigger

Step1 Press the **Setup** soft key.

Step2 Select Capture tab, and then set **Capture** to **Enable**.

Step3 Set **Use Filters as** to **Trigger**.

Step4 Select the **Filters** tab, and then, in the panel on the left side, select **Summary**.

Step5 Select the **Clear All Filters** button to clear any current filter settings.

Step6 In the panel on the left side, select **Byte Pattern**.

Step7 Set the **Use Byte Pattern as** to **Trigger**, and then specify the trigger/filter as described in “Specifying filter settings” on page 95.

Step8 Select the **Capture** tab and specify a **Post-Trigger Size.** This is the amount of data, in MB, to capture after the trigger event occurs. If set to zero, the capture stops immediately after the trigger event.

NOTE:

When capturing packets based on a trigger, the capture buffer saves in wrap-around mode (overwrite the oldest packets with new packets when the buffer becomes full).

Step9 Select the **Capture** toolbar, and then select **Start Capture**.

A message appears in the message bar indicating that the capture has started, and the action key states **Capture Started**.

The capture will begin when the trigger event occurs which will be when the data matches the filter criteria and byte pattern criteria. Captured packets are stored temporarily in the capture buffer. A count of the number of packets processed is provided in the Ethernet result group, in the Capture category.

WARNING: Changing applications or turning OFF the instrument

You will lose the entire contents of the capture buffer if you launch a new application on the port that you are capturing packets on, or if you turn your instrument OFF. To ensure that the packets are stored, save the capture buffer before changing applications or turning the instrument OFF.

Saving or exporting captured packets

After capturing packets, you can save the packets in the buffer to the internal USB drive, or export it to an external USB drive. You can save the entire buffer, or you can indicate that you want to save part of the buffer. You can also optionally turn on gzip compression.

You can also optionally import a pcap file from an external USB drive to analyze it on your unit.

Many factors contribute to the length of time it takes to save a captured file. For example, if you configure a capture for a large buffer size (for example, 256 MB) with small packets (for example, 46 byte ping packets), it will take a long time to save the file due to the large number of packets stored in the buffer. Essentially, the packet density and the capture size determine the length of time it takes to save the packets.

If you are running a TCP Host application, saving captured packets takes a long time; therefore, we recommend stopping the TCP Host application before saving the captured packets.

To save the packets in the capture buffer

Step1 Capture the packets (see “Capturing packets” on page 96).

Step2 Select **Save Capture Buffer**.

The Save Capture File dialog box appears (see Figure 21).

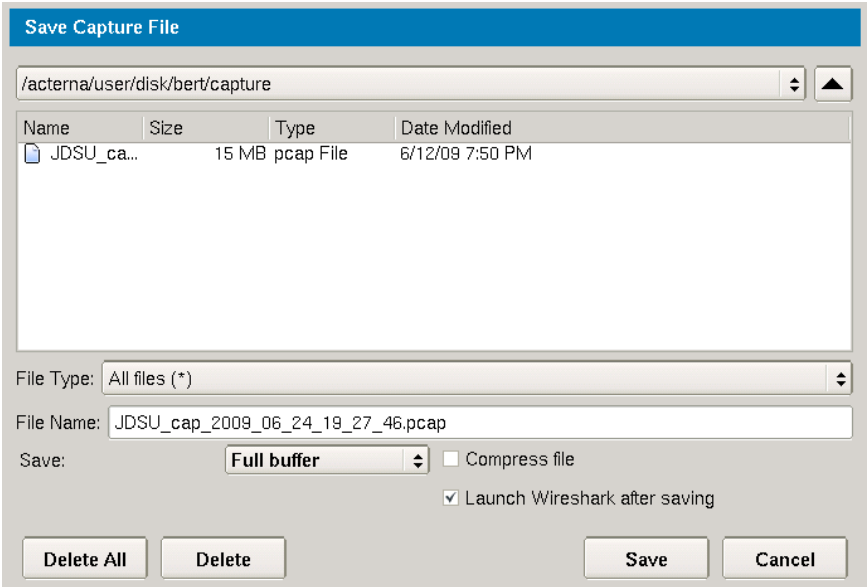


Figure 21 Save Capture File dialog box

Step3 At the top of the dialog box, select one of the following:

To ...	Select this ...
Save the captured packets to the internal USB drive	/acterna/user/bert/disk/capture
Save the captured packets to an external USB drive	/acterna/user/usbflash

Step4 Specify the following settings:

Setting	Parameter
File Type	If you want to see all files stored in the location you selected in step 3, select **All files**; otherwise, accept the default (**Pcap files**).
File Name	If you want to specify a file name instead of accepting the default, type the name using popup keypad. You do not need to specify the .pcap file extension, the instrument will automatically do so for you.
Save	Select one of the following: – If you want to save all of the packets in the buffer, select **Full Buffer**. – If you only want to save some of the packets in the buffer, select **Partial Buffer**.
From	If you indicated that you only want to save part of the buffer (by selecting **Partial Buffer**), specify one of the following: – Start of buffer – End of buffer
Amount	If you indicated that you only want to save part of the buffer (by selecting **Partial Buffer**), specify one of the following: – The number of MB to save (up to 256 MB) – The percentage of the buffer to save
Compress File	By default, the instrument does not compress the file. If you want to save the packets in a compressed (gz) format, select this setting. ***CAUTION!*** *Do not compress the file if you are measuring One Way Delay.*
Launch Wireshark after saving	If you want to launch Wireshark immediately after saving the packets in the capture buffer, select this setting.

Step5 Select the **Save** button at the bottom of the dialog box.

A dialog box appears above the Main screen showing the percentage of the buffer that has been saved. When buffer is saved, the box closes. If you indicated that you wanted Wireshark to launch immediately after saving the buffer, the Wireshark® application appears.

The packets in the capture buffer are saved or exported.



CANCELLING THE SAVE PROCESS:

You can cancel the save process by pressing the **Cancel** button provided on the Save Capture Buffer dialog box. The length of time it take to cancel the save process varies depending on the amount of data stored in the capture buffer. More data in the buffer results in a longer cancellation process.

How long will it take to save the PCAP file?

The length of time it takes to save the PCAP file varies based on a number of factors, including the capture buffer size, the length of the packets captured, the system resources used, and whether or not you chose to compress the file.

Table 10 provides estimates for a 100% full 256 MB buffer, for two packet lengths. The estimates assume you *did not compress the file*, and that you are not running another application on the other port.

Table 10 Estimated time to save a 256 MB PCAP file

Packet Length	Estimated time to save
64 bytes	9 minutes
512 byte frames	8 minutes

Analyzing the packets using Wireshark®

After saving the packets in the capture buffer (to a PCAP file), you can analyze the packets in detail on the instrument using the Wireshark® protocol analyzer. Files exceeding 16 MB should not be analyzed on the instrument; large files should be exported for analysis on another device. If you attempt to analyze a file with more than 50,000 packets, the instrument will alert you that the file should be exported for analysis.

One way to think of the buffer size in relationship to the length of packets is in terms of *density*. A small 1 MB buffer populated with 256 byte packets is not as dense as a 1 MB buffer populated with 64 byte packets, because less 256 byte packets are required to fill the 1 MB buffer. Due to the reduced density of the file, opening the file for analysis take less time. A dense file takes longer to open.



IMPORTANT: Wireshark® Support

JDSU is distributing Wireshark® on the instrument under the GNU General Public License, version 2. It is not a JDSU product. For technical support, go to the product website at www.wireshark.org.

To analyze captured packets

Step1 On the Capture toolbar, select the **Wireshark** action key.

The Open Capture File dialog box appears.

Step2 Navigate to and select the file you want to analyze.

The Wireshark® splash screen appears, then a small dialog box appears while the application loads the packets in the file you selected.

Step3 After the packets are loaded, a screen similar to the one in Figure 22 appears.

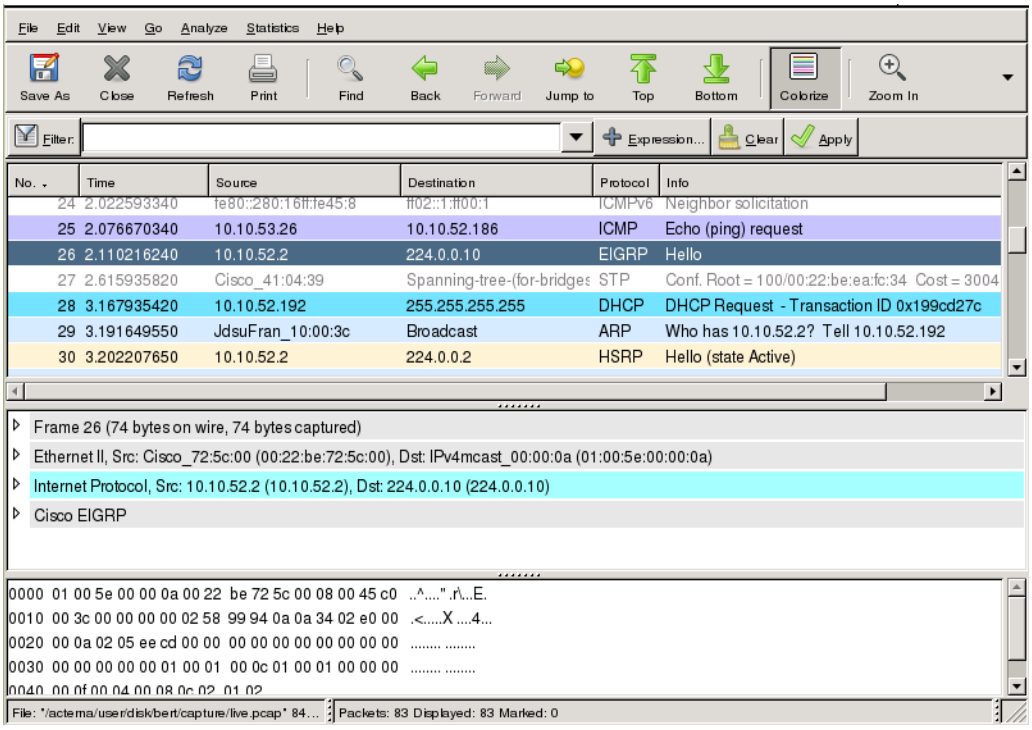


Figure 22 Sample Wireshark® screen

Step4 Use the controls at the top of the screen to locate and evaluate the packets. For technical support and product documentation, go to www.wireshark.org.

You are analyzing captured packets.

Analyzing the packets using J-Mentor

If you want a summarized analysis of the packets, you can use the J-Mentor utility provided on your instrument. The utility is only available for analysis of packets captured on 10/100/1000 Mbps electrical, 100M optical, and 1G optical circuits.

J-Mentor can only be used to analyze PCAP files with 50,000 or less captured packets.

To analyze captured packets

Step1 On the Capture toolbar, select the **J-Mentor** action key.

The Open Capture File dialog box appears.

Step2 Specify the link bandwidth in Mbps. This is the line rate at which you captured the traffic.

Step3 Navigate to and select the file you want to analyze.

Step4 If you want to observe key details for the PCAP file, select **Get PCAP Info**. This is wise if you suspect the file might exceed the 50000 packet limit for analysis on your instrument.

If the file has 50,000 packets (or less), a summary of the data in the file appears, including:

– The number of packets captured
– The file and data size
– The capture duration, start, and stop time
– The data bit and byte rate
– The average packet size
– The average packet rate

If the file has more than 50,000 packets, a message appears indicating that you can not analyze the packets on the instrument. If this occurs, export the PCAP file and analyze it using Wireshark® on your workstation.

Step5 To analyze the packets in the file, select **Analyze**. The utility immediately checks for the following:

– The possible retransmissions of packets
– High bandwidth utilization
– Top talkers
– Detection of half duplex ports
– ICMP frames

After analyzing the packets, the Capture Analysis Summary screen appears, indicating whether issues were found at layers 1 and 2 (the physical and Ethernet layer), layer 3 (the IP layer), or layer 4 (the TCP/UDP layer). Green indicates everything was fine at a particular layer; Red indicates that there were issues identified at that layer. See Figure 23.

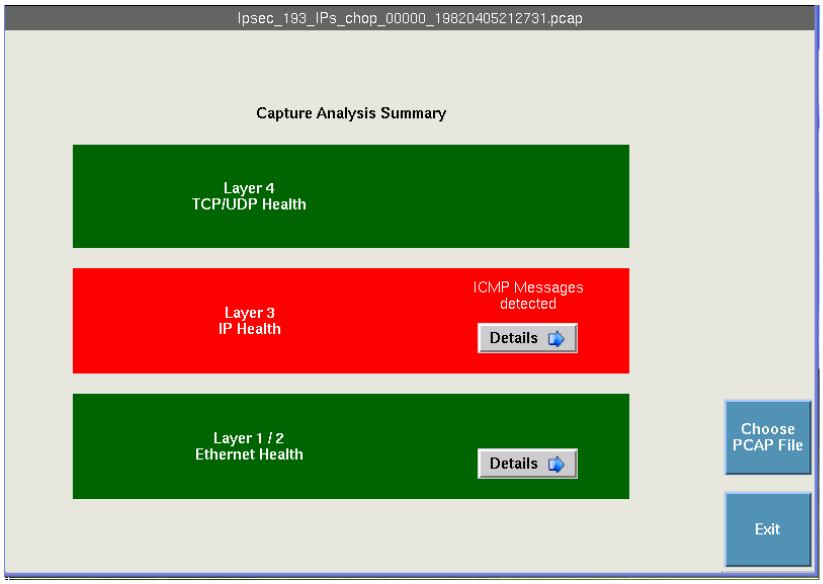


Figure 23 Capture Analysis Summary screen

Step6 Use the **Details** buttons to observe detailed results for each layer. For example, if you want to observe a graph of the network utilization, or a list of all IP conversations, press the Details button for Layer 1 / 2.

Step7 If you want to analyze another PCAP file, select **Choose PCAP File**, and repeat step 3 through step 6; otherwise, select **Exit** to return to the Main Screen.

The packets were analyzed using J-Mentor.

Loop back testing

Loop back testing allows you to transmit traffic from one JDSU Ethernet test set, and then loop the traffic back through a second unit on the far end of a circuit. For details, refer to Chapter 8 “Loop back Testing”.

Inserting errors or pause frames

Action buttons on the Main screen allow you to insert errors and pause frames into the traffic stream. If you turn on a particular error insertion rate, the error insertion continues even after you restart a test or change the test configuration.

– If you selected a 10 Gigabit WAN application, you can also insert SONET/SDH errors and alarms as appropriate. For details, see the *PDH, SONET, SDH, NextGen, and OTN Testing Manual* that shipped with your instrument or upgrade.



NOTE:

Only errors that are applicable to your test appear for selection. For example, IP Checksum errors only appear if you selected a layer 3 or layer 4 test application; TCP/UDP Checksum errors only appear if you selected a layer 4 test application.

To insert errors or pause frames

Step1 If you are inserting pause frames, specify the pause quanta on the Interface tab (see “Specifying interface settings” on page 46); otherwise, proceed to step 2.

Step2 If you are inserting errors, select one of the following error types; otherwise, proceed to step 4:

- Code (optical applications only)
- FCS
- BIT (BERT payload only)
- Pattern (Layer 1 BERT, 1 GigE or 10 GigE applications only)
- IP Checksum (Layer 3 only)
- TCP/UDP Checksum (Layer 4 only). TCP/UDP Checksum errors are only available if you are transmitting fixed BERT patterns. They are not available when transmitting PRB patterns.
- ATP Payload. You must configure the module to transmit an Acterna payload to insert ATP Payload errors.
- Remote Fault - insert on L2 and above (10 GigE, 40 GigE and 100 GigE applications only)
- Local Fault - insert on L2 and above (10 GigE, 40 GigE and 100 GigE applications only)
- Alignment Marker(40 GigE or 100 GigE applications only)
- BIP-8 AM (40 GigE or 100 GigE applications only)
- Block Error on L1 PCS (40 GigE or 100 GigE applications only)

Step3 Do the following:

- Specify the Insertion Style (**Single**, **Burst**, or **Rate**).
- For 40GigE or 100GigE lane errors (**Code**, **Alignment Marker,** or **Bip-8**), select the lane(s) into which the error is to be inserted.
- If you specified Burst, specify the number of errors in the burst, and then select **OK**.
- If you specified Rate, select a rate.

Step4 Do one of the following:

– If you are inserting errors, press the **Error Insert** button.

– If you are inserting pause frames, select the Actions tab, and then press the **Pause Frame Insert** button.

NOTE:

When inserting code errors at a rate of 1E-3 on 10 GigE circuits, the large volume of errors will bring down the Ethernet link.

Per IEEE 802.3ae, a maximum of 16 code violations (invalid synchronization headers) are to be counted per 125 µs. Therefore, inserting a burst of code errors with a quantity greater than 16 will typically be counted as 16 code violations on the receiver.

Error or pause frame insertion starts. If you are inserting errors at a particular rate, the associated button turns yellow. To stop insertion, press the corresponding button again. Error insertion stops, and the associated button turns gray.

Inserting alarms or defects

You can insert multiple types of alarms or defects simultaneously into a single or multiple streams.

To insert alarms or defects

Step1 Using the Test Menu, select the terminate test application for the signal, rate, and payload you are testing (refer to Table 2 on page 26 for a list of applications).

Step2 Connect a cable from the appropriate TX connector to the network's RECEIVE access connector.

Step3 Select the **Laser** button.

Step4 Select an alarm or defect type (**LOBL, LOAML, HI-BER**).

Step5 For alarms that apply to multi-lane applications, specify the number of the lane in which the alarm is to be inserted or select **All**.

Step6 Press the **Alarm Insert** or **Defect Insert** button.

The module inserts an alarm or defect, and the button turns yellow.

To stop insertion (Multiple alarms)

– Press the **Alarm Insert** or **Defect Insert** button again.

When HP-UNEQ or UNEQ-P alarm/defect insertion is stopped, the C2 path overhead byte will be populated by the value configured on the Setup overhead tab.

Alarm or defect insertion stops, and the button turns gray.

Test results associated with the alarm or defect appear in the Status result category.

Measuring round trip delay or packet jitter

You can measure round trip delay or packet jitter by transmitting an Acterna payload. The Acterna payload carries frames with time stamps, enabling the instrument to calculate the delay and jitter. To measure round trip delay, you must use a loopback configuration.

You can measure packet jitter (the difference in one-way-delay as experienced by a series of packets) using either a loopback or an end-to-end configuration. When measuring packet jitter, your unit must receive three or more Acterna frames or packets before measurement begins.

To measure round trip delay or packet jitter

Step1 Use the Test Menu to do one of the following:

– Select the layer 2 or layer 3 traffic terminate test application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Select the **Setup** soft key, and then do the following:

– If you selected a layer 2 traffic application, select the Ethernet setup tab, or if you selected a layer 3 traffic application, select the IP setup tab.

– Select the DATA field to specify that transmitted frames will carry an Acterna payload.

– If you are measuring delay on a 10 Gigabit Ethernet or 10 Gigabit Fibre Channel circuit, verify that the RTD Setup setting is set to **High Precision - Low Delay**.

Step3 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen. If delay through the optic needs to be accounted for, the user needs to enter the latency in the **RTD Optic offset** field, so that it can be subtracted from the delay measurement (enter in microseconds). For more information, see “Optics Expert Mode” in the Getting Started Guide.

Step4 Connect the module to the circuit.

Step5 If you are testing an optical interface, select the **Laser** button.

Step6 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step7 At a minimum, observe the delay and jitter test results in the Ethernet L2 Link Stats or L3 Link Stats category and the L2 Filter Stats or L3 Filter Stats category.

If your delay results (measurements) display “Out of Range”, change the RTD Setup to **Low Precision - High Delay**, and then restart the test.

Round trip delay and packet jitter are measured.

Measuring one way delay

One way delay measurements are measurements of delay *in a single direction* (from a source node to a destination node). They differ from round trip delay measurements because they do not include the cumulative network delays associated with inbound and outbound traffic.

CDMA/GPS receivers

To accurately measure delay in one direction, the time on both nodes must be precisely synchronized. The MSAMs, 5800s, or CSAMs use external CDMA receivers to ensure that both instruments are synchronized, providing measurements that are accurate within +/- 10 µs. A CDMA base station is synchronized to GPS time, and broadcasts this time to the receivers which are connected to your instruments. The receivers provide periodic messages with GPS time, and an accurate 1PPS signal into the BNC connector on your instrument.

A GPS receiver is an alternative to the CDMA receiver. This receiver obtains highly accurate timing information directly from the GPS Satellite. Each MSAM in the system that needs to be synchronized must have its own GPS receiver. The receivers provide periodic messages with GPS time via a DB9 or RJ-45 connector, and an accurate 1PPS signal into the BNC or SMA connector on your instrument.

Whether connected to a CDMA or GPS receiver, your instrument uses the messages and signals to synchronize its internal clock with GPS time. Outgoing packets are then marked with GPS timestamps (see “ATP-GPS test packets” on page 108).

ATP-GPS test packets

When your test instrument is synchronized to GPS time via the CDMA or GPS receiver, it tags outgoing Acterna Test Packets (ATP) with GPS timestamps. The timestamps are required for accurate one way delay measurements. The receiving instrument recognizes these packets and uses them when measuring one way delay.

Network diagram

Figure 24 shows a typical placement of the test instruments and their relationship to the CDMA receivers and base stations. In this configuration, synchronized instrument B measures the delay in traffic received from instrument A, and synchronized instrument A measures the delay in traffic received from instrument B. Each instrument operates in terminate mode, and only measures delay on the *inbound link*.

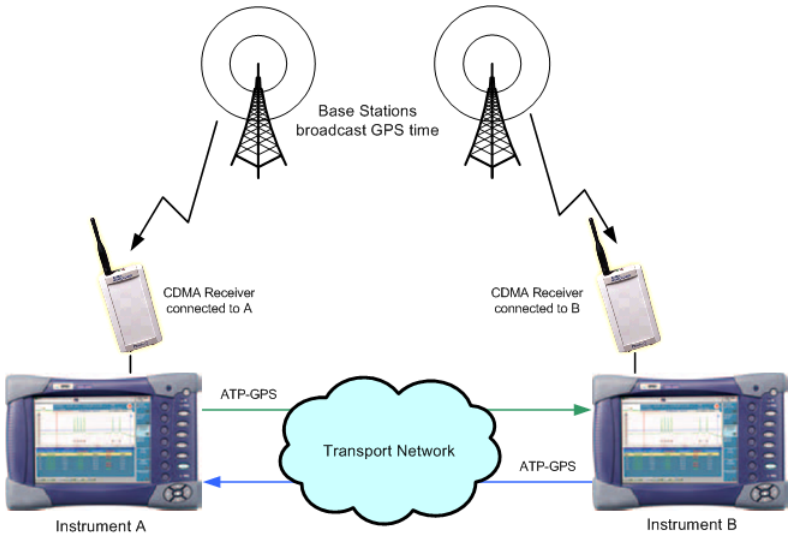


Figure 24 Typical one way delay configuration

Both test ports can be used on the instruments, allowing you to measure one way delay for two different circuits simultaneously. Figure 25 illustrates a configuration used to measure one way delay from A to B, and from A to C. You could also transmit traffic from instruments B and C, and measure delay for both circuits on two independent ports on Instrument A.

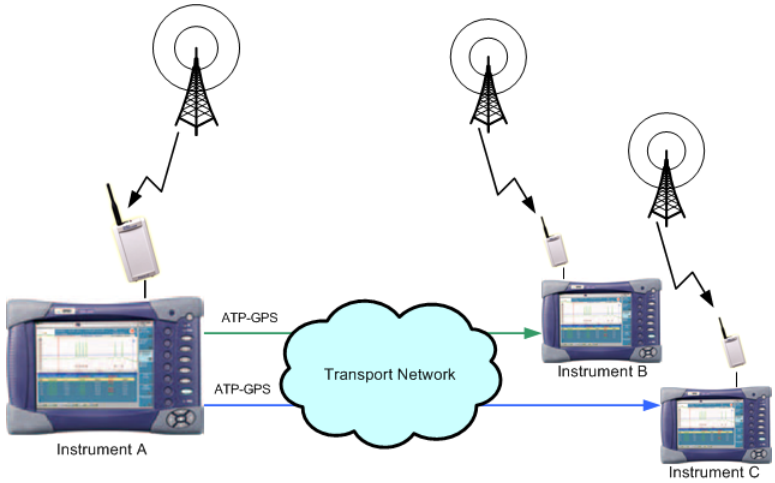


Figure 25 Dual Port configuration

For systems utilizing GPS receivers instead of CDMA receivers, the system is very similar except that the GPS receivers communicate directly with the GPS instead of via terrestrial-based radio.

Things to consider

Before measuring one way delay, consider the following:

- Two GPS synchronized instruments are required to accurately measure one way delay. No communication is required over the Transport network to synchronize the time.
- Both instruments must operate within a CDMA or GPS network to attain GPS synchronization.
- Both ports can be used on the instruments for one way delay testing. In Figure 24 on page 108, one port is used to transmit traffic and measure delay from instrument A to B, and a second port is used to transmit traffic and measure delay from instrument B to A.
- A GPS synchronized instrument and an *unsynchronized* instrument can be used for testing; however, they can not be used to measure one way delay. Neither instrument will provide one way delay measurements.
- Follow the guidelines included in the documentation shipped with the GPS receiver regarding preparation time and hold-over stability to ensure maximum accuracy and stability.
- Acterna traffic can be looped back from an unsynchronized instrument; however, the receiving synchronized instrument will not be able to measure one way delay on the looped back traffic. Round trip delay will be measured instead.
- If instrument B is synchronized, and traffic from instrument A is looped back through B to A, instrument B will measure one way delay (from A to B), but instrument A will only measure round trip delay because it can not measure one way delay on traffic that has travelled *both directions* (in a round trip). Instrument A will measure round trip delay for the returned (looped back) traffic.

  Although it might seem like you can estimate the one way delay from instrument B to instrument A by subtracting the one way delay measurements reported on B from the round trip delay measurements reported on A, the calculation will not be correct. Round trip delay

measurements include internal loopback delays, which vary and depend on the size of looped back frames. Therefore, *the estimate will not be accurate*, and the delay measured will be slightly exaggerated.

– The two instruments used to measure one way delay must use the same BERT software version in order to synchronize timing.
  – Version 10 uses UTC timing, so if measuring one way delay using an instrument running BERT software version 10, the other instrument must also run version 10.
  – Version 11 uses GPS timing, so if measuring one way delay using an instrument running BERT software version 11, the other instrument must also run BERT software version 11.

About the One Way Delay test option and accessory kit

One way delay testing is offered as a test option for your instrument. When you purchase an OWD test option (CDMA or GPS), you receive an accessory kit. The accessory kit can be used with the T-BERD / MTS 5800, 6000A with MSAM, 8000 with DMC, or 8000 with Transport Module, so not all parts are used for a given product.

CDMA Receiver Kit

– Præcis2 CDMA Receiver Package. This package includes a CDMA receiver, AC power adapter, Ethernet cable, DB-9 to RJ-45 adapter, Mag mount 14” antenna, and documentation for the items in the package.
– Antenna stub and magnetic-mount antenna.
– J-Bullet custom attenuator
– BNC (male) to BNC (male) cable
– SMA to BNC Adapter
– SMA to BNC cable
– SMA to SMA cable
– RS-232 Serial cable
– RS-232 to USB converter
– Serial DB-9 to RJ-45 cable

GPS Receiver Kit

– Spectrum Instruments TM=4M GPS receiver
– Antenna
– J-Bullet attenuator, 500 ohm - JDSU
– BNC (male) to BNC (male) cable
– SMA to BNC Adapter
– SMA to BNC cable
– SMA to SMA cable
– RS-232 Serial Cables
  – DB9 (female) to RJ-45 (1)
  – DB9 to DB9 (1)
– RS-232 to USB converter
– Documentation and software for items in the package

Step 1: Connecting the receivers to your instruments

Before measuring one way delay, you must connect the receivers (CDMA or GPS) to each of the test instruments. The CDMA receivers will communicate with each other to establish synchronization. The GPS receivers will establish synchronization by using the common signal from the GPS satellite.

Connecting the CDMA Receiver

Figure 26 illustrates each of the required connections for a CDMA receiver connected to aT-BERD/MTS 5800 or a MTS6000 or MTS8000v2 base unit with a CSAM or MSAM module.

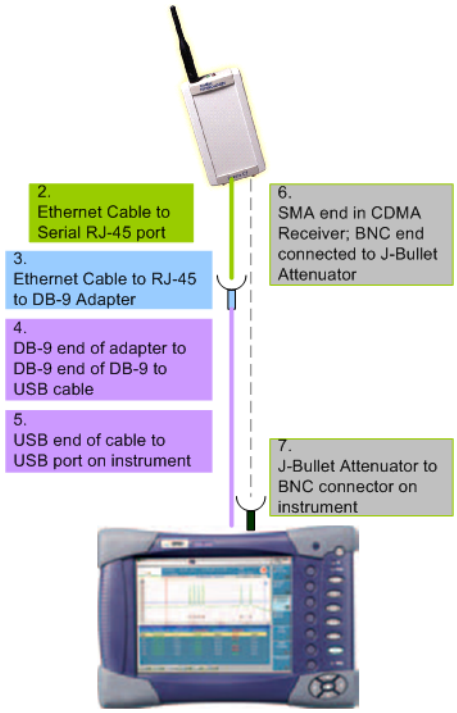


Figure 26 CDMA connection for one way delay measurements

To connect a CDMA receiver to your instrument

Step1 Connect the ToD signal between the CDMA receiver and the MST6000 or MST8000.

a Connect one end of the Ethernet cable to the serial RJ-45 port of the CDMA receiver.

b Connect the other end of the Ethernet cable to the RJ-45 to DB9 adapter.

c Connect the other end of the cable to the instrument:

– If using a DMC in an 8000v1 base unit, connect the DB9 adapter to the instrument.

– If using a CSAM or MSAM with a 6000A or 8000v2 base unit, do the following:

i. Connect the DB9 end of the RJ-45 to DB9 adapter to the DB9 to USB cable.

ii. Connect the USB end of the DB9 to USB cable to a USB port on your instrument.

d If using a CSAM, connect a SMA to SMA cable from “1PPS” output jack on the CDMA receiver to a SMA to SMB adapter and then to the CSAM’s “CLK OUT/1PPS” port.

Step2 Verify that your instrument is synchronized with GPS time by checking the CDMA Sync and 1PPS Sync LEDs. When synchronized, the LEDs will be illuminated.

Step3 Repeat step 1 through step 2 on the second instrument.

The receivers are connected to your instruments, and the instruments are synchronized with GPS time.

Connecting the GPS receiver

GPS is increasingly being used as a timing reference because it available almost everywhere providing a common reference between various field locations. This provides the capability of one-way delay measurements with greater accuracy than are possible utilizing existing round-trip delay measurements.

A GPS receiver provides accurate ToD and 1PPS signal, which, when averaged over a long time period, provide very precise signals that can be used to create common timestamps and as reference clock for other precision system measurements. The GPS receiver provides a Time of Day (ToD) and a 1PPS signal which are used to generate accurate time stamps that are encoded into the data transmitted between the local and remote instruments.

To connect the GPS receiver to your instrument

Step1 Connect the 1PPS signal between the GPS receiver and the instrument.

- If you are connecting to a MSAM v1, connect the BNC to BNC cable from “OUT B” on the GPS receiver to the J-Bullet attenuator, and then connect the J-Bullet attenuator to the “EXT REF” connector on your instrument (see Figure 27 on page 113, Figure 28 on page 113, or Figure 29 on page 114).
- If you are connecting to a MSAMv2, connect the BNC to SMA cable from “OUT B” on the GPS receiver to the “EXT REF” connector on your instrument (see Figure 33 on page 116, Figure 34 on page 116, or Figure 35 on page 117).
- If you are connecting to a 5800v1, connect the BNC to SMA cable from “OUT B” on the GPS receiver to the “EXT REF” connector on your instrument (see Figure 30 on page 114).
- If you are connecting to a 5800v2, connect the BNC to SMA cable from the “OUT B” on the GPS receiver to the SMA Timing Cable Adapter’s CLK2 connector, which is connected to the “EXT CLK” connector on your instrument (see Figure 31 on page 115).
- If you are connecting to a CSAM, connect the SMA to SMB adapter to the CSAM’s “CLK OUT/1PPS” port, then connect the SMA to BNC cable from the adapter to “OUT B” on the GPS receiver.

Optional. Connect the DB9 to USB serial cable from the Control Port on the GPS receiver to a PC.

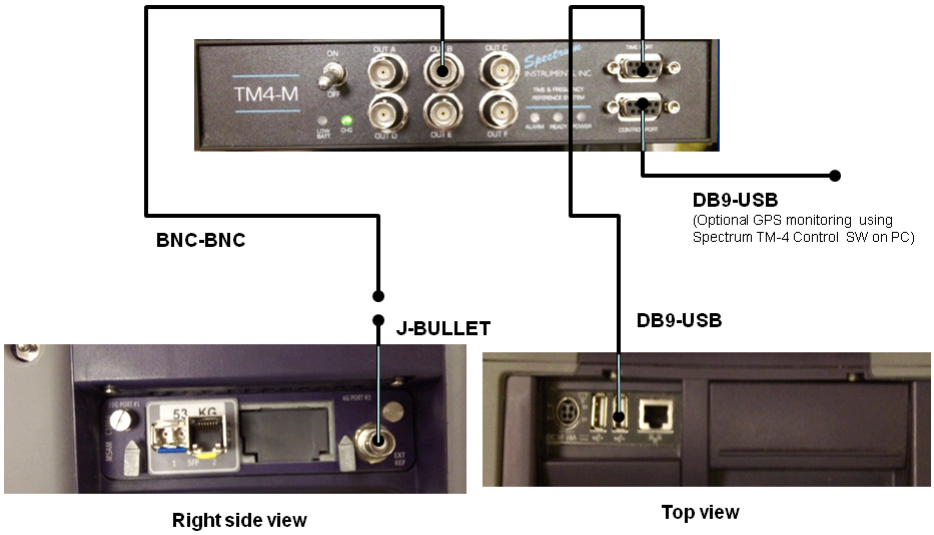


Figure 27 GPS Connection Diagram- MSAMv1 w/ MTS6000A

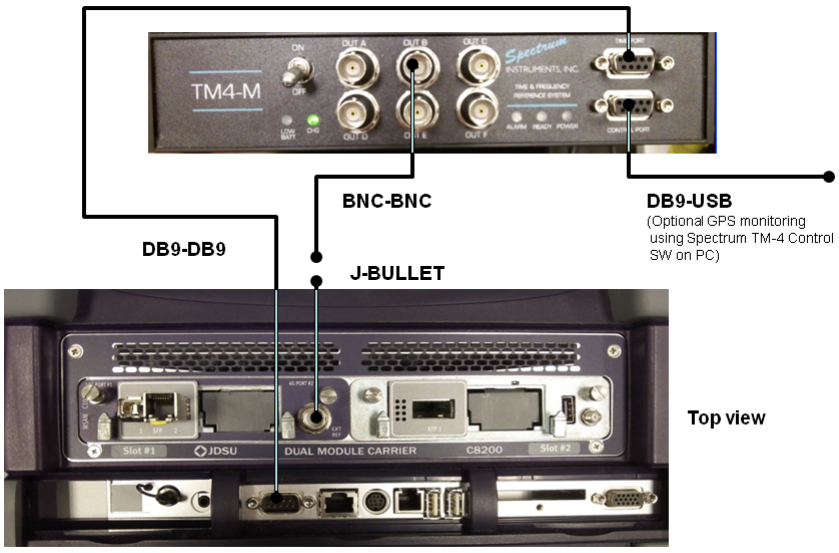


Figure 28 GPS Connection Diagram - MSAM v1 in MTS8000v1

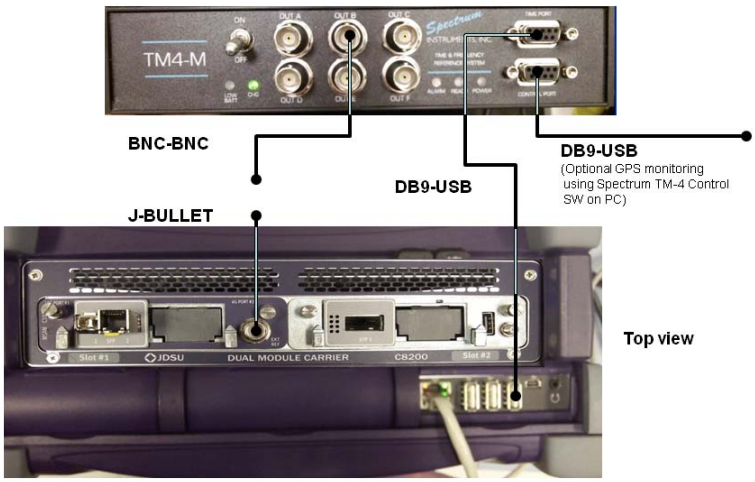


Figure 29 GPS Connection Diagram - MSAM v1 in MTS8000v2

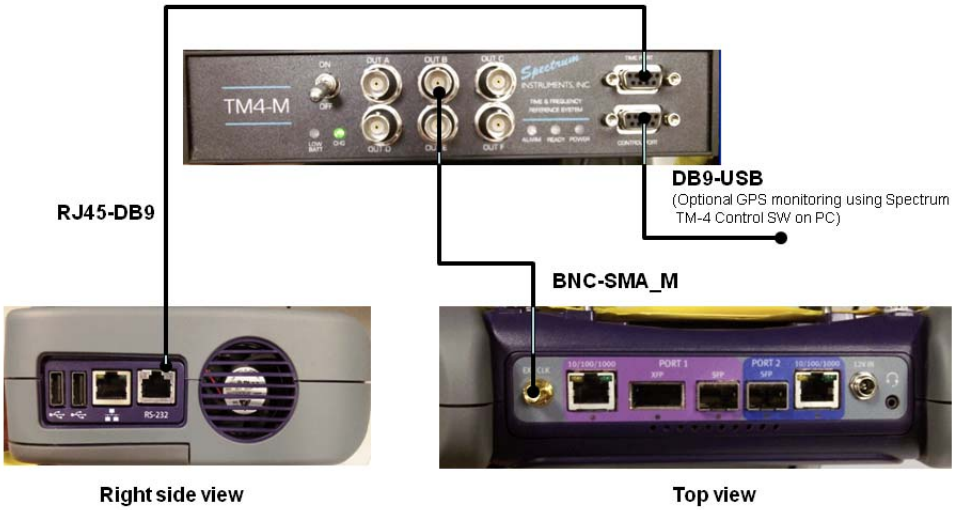


Figure 30 GPS Connection Diagram - 5800v1

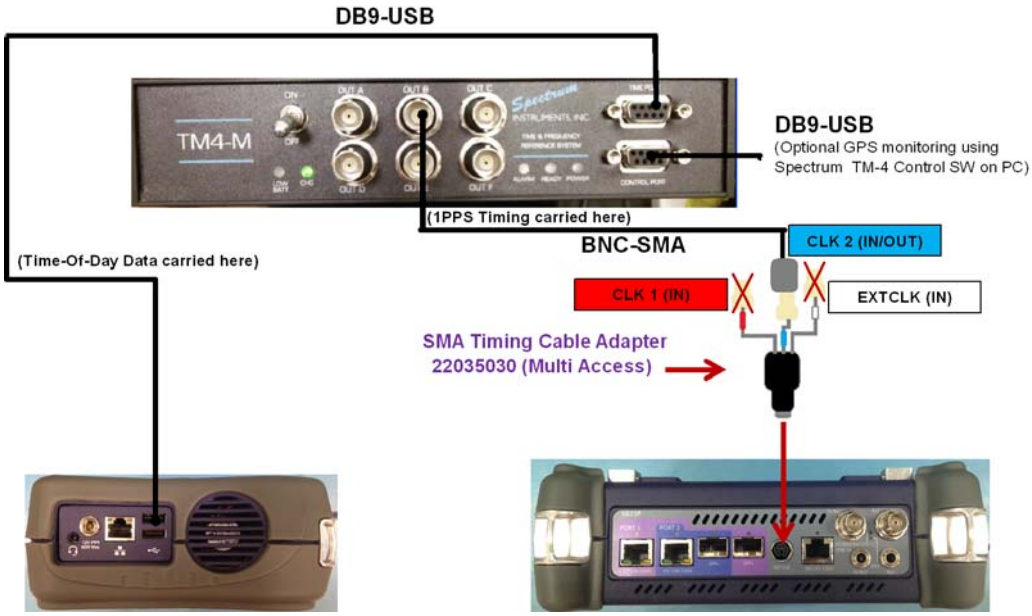


Figure 31 GPS Connection Diagram - 5800v2

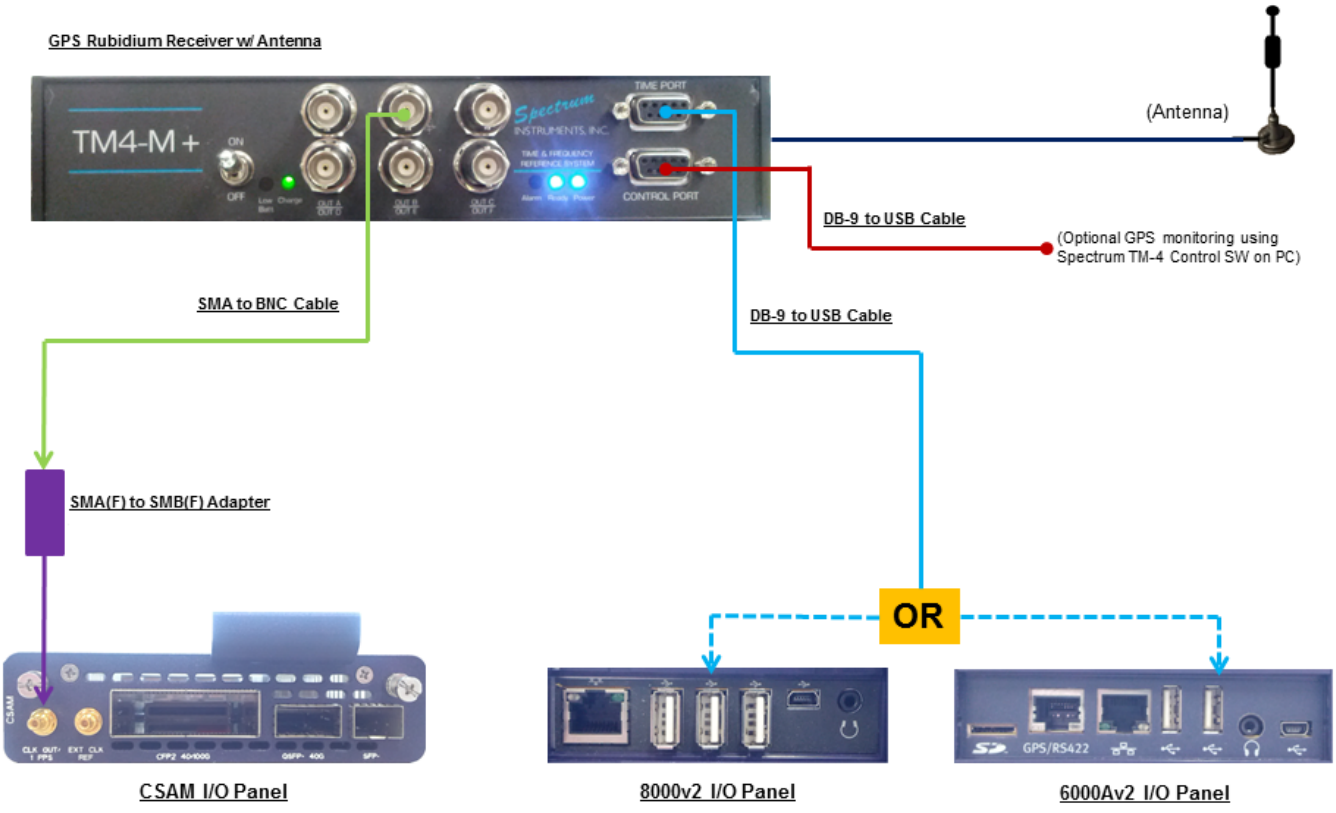


Figure 32 GPS Connection Diagram - CSAM

Step2 Connect the ToD signal between the GPS receiver and the instrument.

- For an 8000v1, connect the DB9-DB9 cable from the “Time Port” on the GPS receiver to the DB9 connector on the T-BERD/MTS 8000, 6000A, and 5800 (see Figure 28 on page 113 or Figure 34 on page 116).
- For a 5800v1, connect the DB9 to RJ-45 cable from the “Time Port” on the GPS receiver to the RJ-45connector on the 5800 (see Figure 30 on page 114).
- For a 5800v2, 6000A or 8000v2, connect the DB9 to USB cable from the “Time Port” on the GPS receiver to the USB port on the 6000A or 8000 (see Figure 27 on page 113, Figure 29 on page 114, Figure 31 on page 115, Figure 32 on page 115, Figure 33 on page 116, or Figure 35 on page 117).

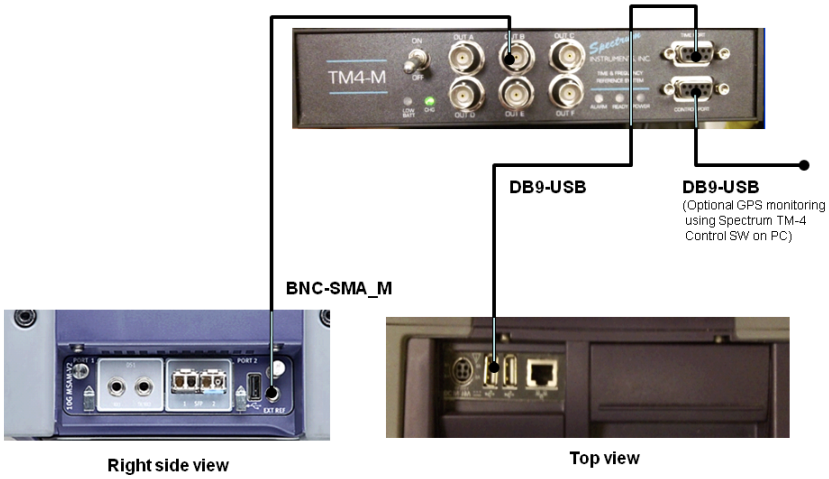


Figure 33 GPS Connection Diagram - MSAMv2 w/ MTS6000A

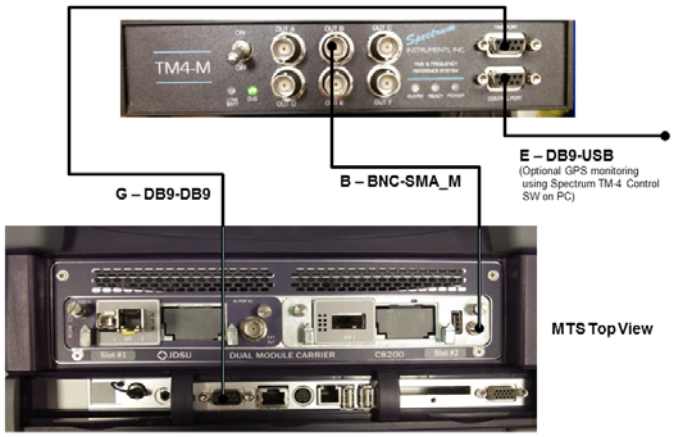


Figure 34 GPS Connection Diagram - MSAM v2 in MTS8000v1

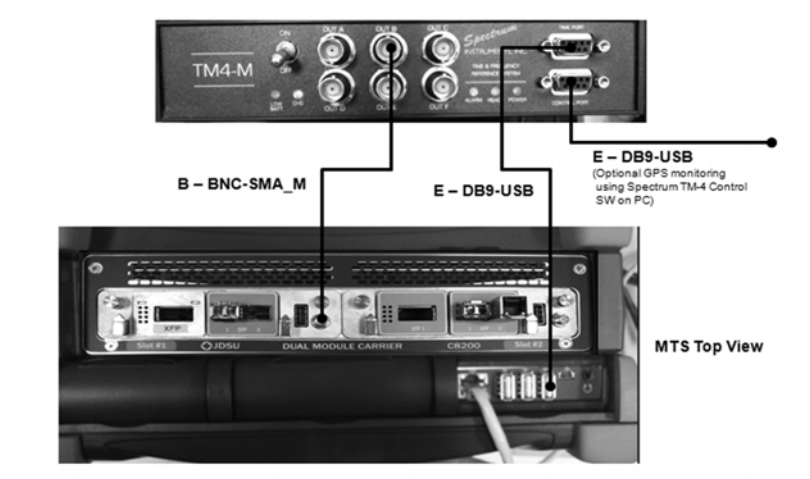


Figure 35 GPS Connection Diagram - MSAM v2 in MTS8000v2

Step3 Repeat step 1 and step 2 on the second instrument.

Step4 Verify that it is synchronized with GPS time by checking the GPS Sync and 1 PPS Sync LEDs. When synchronized, the LEDs will be illuminated.



The 1PPS minimum pulse width that can be detected is 20µs.

The GPS receivers are now connected for OWD testing.

Step 2: Measuring one way delay

Two synchronized instruments are required to measure one way delay. On both instruments, you select a traffic application for the line rate of the circuit you are testing, and you configure the traffic to carry an Acterna payload. This payload carries frames with time stamps, enabling the receiving instrument to calculate the delay.

To measure one way delay

Step1 On each instrument, use the Test Menu to do one of the following:

– Select the layer 2 or layer 3 traffic terminate test application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 On each instrument, select the **Setup** soft key, and then do the following:

a If you selected a layer 2 traffic application, select the Ethernet setup tab, or if you selected a layer 3 traffic application, select the IP setup tab.

b Select the **Data** field to specify that transmitted frames will carry an Acterna payload. The payload can be populated with a BERT pattern or Fill Byte pattern.

c Select the **Interface** tab, and then on the **CDMA/GPS Receiver** tab, do the following:

– Enable the **CDMA or GPS** receiver.

– If using a CDMA receiver, choose a **Channel Set**. The selections the vary based on which CDMA receiver is being used.

Step3 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

Step4 Connect the instruments to the circuit. For details, refer to the Getting Started manual that shipped with your instrument or upgrade.

Step5 If you are testing an optical interface, select the **Laser** button.

Step6 Select the **Restart** button.

Step7 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated on each instrument.

Step8 At a minimum, observe the one way delay test results in the Ethernet L2 Link Stats or L3 Link Stats category and the L2 Filter Stats or L3 Filter Stats category. CDMA/GPS Receiver results are also available for review.

You have measured one way delay.

Measuring service disruption time

You can use two instruments in an end-to-end configuration to measure the service disruption (SD) time resulting from a switch in service to a protect line. The traffic originating unit must transmit a constant rate of traffic to obtain accurate measurements.

By default, all units stop Tx traffic when they detect a break in the Rx link. This means that recorded Service Disruption times will include the time that the Rx line was down plus the time needed to restart traffic and auto-negotiate (if enabled).

With some optical applications (100M, 1G and 10G LAN), configured with full duplex communication, it is possible to decouple the Rx line from the Tx line and prevent this condition from occurring, thus achieving a much more accurate Service Disruption measurement. If the unit is capable of decoupling there will be an active Decouple Tx/Rx option next to the Reset Service Disruption Test button on the Actions panel at the bottom of the main screen.

NOTE:

Decoupling the Tx and Rx links is only applicable to the Service Disruption measurement on Ethernet interfaces (except L4 TCP Wirespeed). In order for the decoupling to occur, the circuit must support ethernet service disruption.

Take decoupled SD measurements exclusive of other measurements as the decoupling has varying affects on other measurements.

Disable the decoupling before making any other measurements or analysis.

When using the 400G/100G module, the CFP FIFO reset is bypassed to get more accurate measurements in decouple mode. (More details in “*Optics Expert Mode” in the Getting Started Guide*.)

To measure service disruption time

Step1 Using the Test Menu, do one of the following:

– If you are using two Transport Modules, on both units, use the Test Menu to select the layer 2 or layer 3 traffic terminate test application for the interface you are testing (refer to Table 2 on page 26 through Table 3 on page 27 for a list of applications).

Step2 Configure the traffic originating unit to transmit a constant load of traffic. If you are using a Transport Module to generate traffic, the load is configured on the Traffic setup tab. For instructions on configuring a constant load of traffic to transmit to another instrument, see "Transmitting a constant load" on page 64.

Step3 If you are using a Transport Module or Transport Module to originate traffic, and you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

Step4 Connect the near and far end units to the circuit under test. When connecting Transport Modules to the circuit, blinking LEDs on the connector panels indicate which connectors to use for your test.

Step5 If you are testing on an optical circuit, on the traffic originating unit, select the **Laser** button.

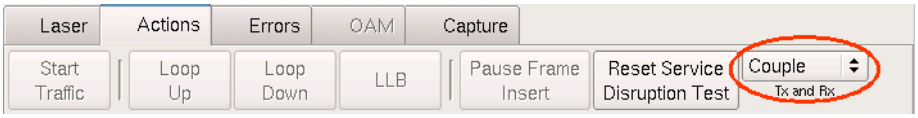
Step6 On the instruments, verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step7 On the traffic originating unit, do the following:

a Start traffic.

b If you are using a Transport Module or Transport Module to transmit traffic, clear the service disruption time by selecting the **Reset Service Disruption Test** button on the Main screen.

c If desired, **Enable** Decouple Tx and RX.



The coupling selection is only available if testing full duplex 100M, 1G, or 10G LAN optical circuits, or on 40G/100G module in OTU4 Ethernet Client and Line Rate Ethernet.

Step8 Initiate the switch to the protect line.

Step9 Observe the service disruption result in the Ethernet L2 Link Stats result category.

You have measured service disruption time.

OAM service and link layer testing

You can position the instrument at various endpoints in a Maintenance Domain (MD) or Maintenance Association (MA) area to verify that no trunk problems occur per ITU-T Rec. Y.1731 and IEEE 802.1ag.

You can also use the instrument to verify point-to-point link layer performance per IEEE 802.3ah. You can observe results associated with your test in the OAM result category. For details, refer to "Ethernet OAM Service OAM results" on page 369 of Chapter 13 "Test Results".

Service layer features

When using your instrument for service layer OAM testing, you can do the following:

- Specify the Maintenance Domain (MD) level, Maintenance Entity Group (MEG) End Point IDs, and Maintenance Association (MA) IDs.
- Specify the Continuity Check Message (CCM) transmission rate (non-MPLS).
- Specify the CCM and LBM Multicast address when running non-MAC-in-MAC applications.
- Choose from a variety of defect and continuity detection options -Continuity Verification (CV), Fast Failure Detection (FFD), Backward Defect Indication (BDI) and Forward Defect Indication (FDI)- for MPL S applications.
- Specify thresholds for declaring a loss of continuity (LOC) if the number of consecutive missing CCM exceeds the number of messages expected within the calculated interval. This state may be used by Maintenance End Point devices to initiate a switch to a protect line.

  NOTE: Service OAM testing is not applicable with 40G/100G Transport Module.
- Fast OAM “heartbeat” messages (CCM/FFD) for
  - Y.1731 (OAM for Ethernet)
  - G.8114/G.8113.1 (OAM for T-MPLS)
  - Y.1711 (OAM for MPLS)
- MEP Discovery – identifies various EVCs (Ethernet Virtual Circuits), such as a VLAN or Q-in-Q in the network, to verify that the correct MEPs are in the correct MD (maintenance domain) level and within the correct EVC.

Link layer features

When using your instrument for link layer OAM testing, you can do the following:

- Identify a discovered OAM as a peer, matching all setups to its detected capabilities.
- Indicate whether you want the instrument to serve in an active or passive role.
- Specify the Vendor OUI (Organizationally Unique Identifier) for the instrument.
- Indicate whether the instrument will advertise that it provides unidirectional support for failure detection, remote loopback, link events, and variable retrieval.
- Indicate whether you want the instrument to generate link faults, dying gasps, and critical events.
- Indicate whether you want the instrument to issue a remote loopback command to place its peer in loopback mode if the instrument is in active mode and its peer is capable of remote loopbacks.

  NOTE: Link layer OAM testing is not applicable with 40G/100G Transport Module.

Specifying OAM settings

OAM settings are specified for the traffic originating instrument on the OAM setup tab when configuring Layer 2 Traffic tests in Terminate mode.

To specify OAM settings

Step1 If you haven’t already done so, use the Test Menu to select the Layer 2 Traffic test application for the interface you are testing. Refer to Table 2 on page 26 for a list of layer 2 applications.

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see "Specifying interface settings" on page 46).

Step3 Specify the settings that characterize the transmitted traffic (see "Specifying Ethernet frame settings" on page 49), and then specify the filter settings (see "Specifying Ethernet filter settings" on page 56).

Step4 Select the OAM tab. The pane on the left of the tab groups the link settings (L-OAM) and service settings (S-OAM).

Step5 To specify link OAM settings, do the following:

a In the left pane, under L-OAM, select **Local Config**, then specify the following settings:

Setting	Parameters
Link OAM State	If you want to enable link OAM, select **On**; otherwise, select **Off**.
Mode	Select one of the following: – **Active**. Select Active if you want the instrument to automatically discover and monitor the peer on the link. – **Passive**. Select Passive if you want the peer to initiate the discovery process.
Vendor OUI	Specify the Vendor OUI (Organizationally Unique Identifier) for the instrument.
Unidirectional	Select this setting if you want to advertise that the instrument is capable of sending OAM PDUs when the receiving path is non-operational.
Remote Loopback	Select this setting if the instrument supports OAM remote loopback mode.
Vendor Specific Info	Enter the value used to differentiate the vendor's product models or versions. Entry of a value is optional.
Link Events	Select this setting if the instrument supports Link Event interpretation.
Variable Retrieval	Select this setting if the instrument can send Variable Response OAM PDU.
Max PDU Size	Specify the largest OAM PDU size.

b In the left pane, under L-OAM, select **Events**, then specify the following settings:

Setting	Parameters
Link Fault	Select this setting if you want to indicate to the peer a fault has occurred.
Critical Event	Select this setting if you want to indicate to the peer that a critical event has occurred.
Dying Gasp	Select this setting if you want to indicate to the peer that an unrecoverable local failure condition has occurred.
Errored Symbol Period Event	
Event Window (total symbols)	Specify the number of symbols that can be received in the period on the underlying physical layer.

Setting	Parameters
Event Threshold (errored symbols)	Specify the number of errored symbols in the window specified required for an error to be declared.
Errored Frame Event	
Event Window (100ms intervals)	Specify the duration of the frame window in terms of the number of 100 ms period intervals. For example, 2 indicates that the window spans a 200 ms period interval.
Event Threshold (errored frames)	Specify the number of detected errored frames required within the window specified for an error to be declared
Errored Frame Period Event	
Event Window (total frames)	Specify the duration of the window in terms of frames.
Event Threshold (errored frames)	Specify the number of frame errors that must occur in the window to declare an error.
Errored Frame Second Summary Event	
Event Window (100ms intervals)	Specify the duration of the period in terms of the 100 ms interval.
Event Threshold (errored sec)	Specify the number of errored frame seconds that must occur in the window to declare an error.

Step6 To specify service OAM settings, do the following:

a In the left pane, under S-OAM, select **CCM**, and then specify the following settings:

Setting	Value
Continuity Checking	Select one of the following: – **On.** Select **On** if you intend to test for loss of continuity (LOC). – **Off.** Select **Off** if you do not intend to test for loss of continuity.Go to step b.
LOC Threshold (messages)	Specify the number of messages that must be received within the calculated interval (see "CCM Rate").
CCM Rate	Specify the rate at which the instrument will transmit CCM messages. The instrument will transmit CCM messages at the rate specified; if it does not receive the number of messages back that you specify as the threshold within the calculated interval (CCM Rate times LOC Threshold (messages)), the instrument declares a loss of continuity (LOC).
CCM Type (non-MAC-in-MAC applications only)	Select one of the following: – **Unicast.** Select **Unicast** to send CCMs to its destination address. – **Multicast.** Select **Multicast** to send CCMs to a reserved multicast MAC address. This setting does not appear when running Mac-in-Mac applications.

Setting	Value
MEG End Point ID	Specify the Maintenance Entity Group End Point ID for the instrument. The instrument encodes the ID that you specify in the CCMs that it sends to its peer.
Peer MEG End Point ID	Specify the Maintenance Entity Group End Point ID for the instrument's peer. The instrument uses the peer ID that you specify to indicate whether CCMs are detected with unexpected MEG End Point IDs.
Maintenance Domain Level	Specify the level for the Maintenance Domain (MD). The instrument uses the level that you specify to indicate whether CCMs for unexpected lower levels are detected in the traffic stream.
Specify Domain ID	Select one of the following: – If you are testing per IEEE 802.1ag, select **Yes**. – If you are testing per ITU-T Rec. Y.1731, select **No**.
Maintenance Domain ID (Specify Domain ID must be Yes)	The instrument uses the ID that you specify to indicate whether CCMs are detected with different IDs. If you indicated that you want to specify a domain ID, enter the ID using from 1 - 43 characters. The combined length of the Maintenance Domain ID field and the Maintenance Association ID field may not exceed a total of 44 bytes. Modifying either field may thus result in the other being truncated in order to meet this requirement.
Maintenance Association ID	The instrument uses the ID that you specify to indicate whether CCMs are detected with different IDs. If you indicated that you want to specify a domain ID, Specify the Maintenance Association ID, using up to 43 characters. The combined length of the Maintenance Domain ID field and the Maintenance Association ID field may not exceed a total of 44 bytes. Modifying either field may thus result in the other being truncated in order to meet this requirement.

b In the left pane, under S-OAM, select **AIS**, and then specify the following settings:

Setting	Parameters
AIS State	If you want to test AIS, select **On**; otherwise, select **Off**. Go to step c.
Maintenance Domain Level	Specify the level for the Maintenance Domain (MD). The instrument will indicate whether AIS for the specified level are detected in the traffic stream.
AIS Rate	Specify the rate at which the instrument will transmit AIS.
AIS Type (non MAC-in-MAC applications only)	Select one of the following: – **Unicast**. Select Unicast to send AIS to its destination address. – **Multicast**. Select Multicast to send AIS to a reserved multicast MAC address. This setting does not appear when running Mac-in-Mac applications.

c In the left pane, under S-OAM, select **LBM/LBR**, and then specify the following settings:

Setting	Value
LBM/LBR (ping)	Select one of the following: – **On.** Select **On** if you intend to verify connectivity by transmitting ping messages. – **Off.** Select **Off** if you do not intend to verify connectivity. Go to step d.
Maintenance Domain Level	Specify the level for the Maintenance Domain (MD). The instrument uses the level that you specify to indicate whether loopback replies (LBRs) for unexpected lower levels are detected in the traffic stream.
LBM Type (non-MAC-in-MAC applications only)	Select one of the following: – **Unicast.** Select **Unicast** to send CCMs to its destination address. Unicast is the default setting. – **Multicast.** Select **Multicast** to send CCMs to a reserved multicast MAC address. This setting does not appear when running MAC-in-MAC applications.

d In the left pane, under S-OAM, select **LTM/LTR**, and then specify the following settings:

Setting	Value
LTM/LTR (trace)	Select one of the following: – **On.** Select **On** if you intend to verify connectivity by transmitting trace messages. – **Off.** Select **Off** if you do not intend to verify connectivity. Go to step 7
Maintenance Domain Level	Specify the level for the Maintenance Domain (MD). The instrument uses the level that you specify to indicate whether loopback replies (LBRs) for unexpected lower levels are detected in the traffic stream.

Step7 Press **Results** to return to the Main screen.



NOTE:

Before turning the laser ON (if you are testing on an optical circuit), and starting traffic, be certain to verify that the filter settings on the receiving instrument match the settings for transmitted traffic on the traffic originating unit. For example, be certain to specify the same protocol or data length for transmitted traffic on the traffic originating unit, and filtered traffic on the receiving unit.

Step8 If testing on an optical circuit, at the bottom of the main page, select the Laser tab on the action bar then click **Laser** to On.

Step9 Select the Action tab on the action bar, and then click **Start Traffic**.

Step10 Select the OAM tab on the action bar and then click BDI and/or FDI to begin insertion of Backward and/or Forward Defect Insertion.

The OAM settings are specified.

Turning AIS or RDI analysis ON

If you want to analyze traffic for AIS or RDI during the course of your test, you must turn AIS or RDI analysis ON.

To turn AIS or RDI analysis ON

Step1 On the Main (Results) screen, select the **OAM** action panel.

Step2 Select **AIS** or **RDI**.

AIS or RDI analysis is on, and your instrument will indicate whether AIS or RDIs have been detected. When AIS analysis is On, pressing Restart will not interrupt analysis; you must turn AIS analysis off to clear AIS test results.

Sending LBM or LTM messages

If you turned LBM/LBR or LTM/LTR on when you configured the OAM settings, you can send LBM ping messages or LTM trace messages, and then ensure that you receive LBR or LTR messages to verify OAM connectivity.

To send an LBM or LTM message

Step1 On the Main screen, select the **OAM** action panel.

Step2 Select **LBM** or **LTM**.

The instrument sends an LBM or LTM, and reports the number of transmitted LBM or LTM frames, and received LBR or LTR frames in the OAM result category.

MAC-in-MAC testing

If you purchased the MAC-in-MAC option for your instrument, a series of MAC-in-MAC (MiM) applications are available which allow you to transmit and analyze unicast layer 2 Ethernet traffic carried on a PBB (Provider Backbone Bridged) trunk. When configuring the traffic, you specify a backbone destination address (B-DA), backbone source address (B-SA), and backbone tag (B-TAG) which designate the path for the backbone frame to the destination.You can also characterize the customer frame (carried in the backbone frame) by specifying the frame type, I-TAG settings, encapsulation settings, and frame size.

When analyzing MiM traffic, you can set up a filter on the receiving instrument to observe test results for traffic sharing the same B-TAG (tag settings for the backbone frame), I-TAG (tag settings for the customer frames), customer frame settings such as the frame type, encapsulation values, and the pattern carried in the customer frame payload.

Understanding MAC-in-MAC test results

When the instrument is configured for MiM testing, a subset of the standard layer 2 test results is provided for the backbone and customer frames (see “CPRI/OBSAI test results” on page 341 of Chapter 13 “Test Results”). When observing results for the backbone frames, B-TAG and I-TAG information is also provided.

Understanding the MAC-in-MAC LEDs

In addition to the standard LEDs provided for layer 2 Ethernet testing, a PBB Frame Detect LED is available which indicates whether the unit has detected MiM traffic on the circuit.

Configuring layer 2 MAC-in-MAC tests

Before transmitting or analyzing traffic on a PBB trunk, you must select the appropriate MAC-in-MAC (MiM) test application, specify interface settings, specify frame and frame filter settings, and then configure the traffic load. Instructions are provided in this section for the following:

– "Specifying interface settings" on page 126
– "Specifying Ethernet frame settings" on page 126
– "Specifying Ethernet filter settings for MiM traffic" on page 129
– "Specifying traffic load settings" on page 130

Specifying interface settings

Before you transmit layer 2 MiM traffic, you can specify interface settings that provide the speed and duplex settings for 10/100/1000 Ethernet traffic, indicate how you want the unit to handle flow control, provide the pause quanta for transmitted pause frames, and identify all traffic originating from your particular Transport Module.

For detailed instructions on specifying these settings, refer to "Specifying interface settings" on page 46.

Specifying Ethernet frame settings

Before you transmit layer 2 Ethernet traffic over a PBB trunk, you can specify the frame characteristics of the traffic, such as the backbone source address, destination address, tag settings, and payload (Acterna test frames or BER patterns).

To specify Ethernet frame settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 3 on page 27 for a list of MiM applications.

Step2 Select the **Setup** soft key, and then select the **Ethernet** tab. A graphical display of a MiM frame appears.

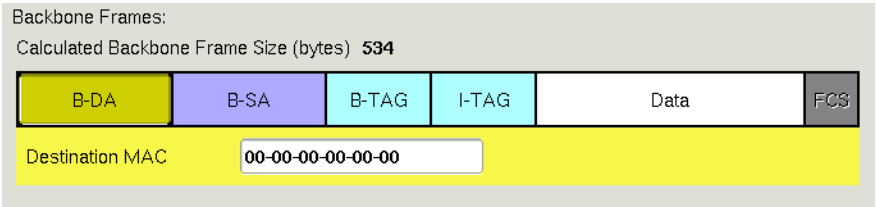


Figure 36 Backbone frame (MiM Traffic application)

Step3 In **Frame Size (Bytes)**, select one of the seven IEEE recommended frame lengths, Random (to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations), or enter a specific Jumbo, Undersized, or User Defined frame length.

If you selected Random or EMIX, use the **Configure** button to specify user-defined random frame sizes, including Jumbo, or select Reset to transmit frames of randomly generated sizes based on the seven RFC 2544 frame length recommendations. EMIX also adds the EMIX Cycle Length field that controls how many frame entries are sent, in order, before cycling back to the first frame entry and repeating. To define the number of frame entries, enter a number between 1 and 8.



NOTE:

Undersized is available in the Frame Size menu if the TX payload is something other than Acterna with BERT payload.

Step4 Use the graphical display of a backbone frame (illustrated in Figure 36 on page 126) to specify the following:

Frame Label	Setting	Value
B-DA	Destination MAC	Enter the destination address using a 6 byte hexadecimal format.
B-SA	Source Type	Select **Factory Default** or **User Defined**.
	User MAC	If you specified User Defined, enter the source MAC address using a 6 byte hexadecimal format.
B-TAG	B-Tag VLAN ID	Enter the ID for the backbone VLAN used as the path to the destination.
	B-Tag Priority	Enter the priority code point (PCP) ID representing the type of service the transmitted traffic is emulating.
	B-Tag DEI BIT	Indicate whether the traffic is drop eligible by setting the DEI bit for the transmitted traffic.
I-TAG	I-Tag Priority	Enter the priority code point (PCP) ID representing the type of service the transmitted traffic is emulating.
	I-Tag DEI Bit	Indicate whether the traffic is drop eligible by setting the DEI bit for the transmitted traffic.
	I-Tag UCA Bit	Indicate whether you want to use the customer address by setting the bit.
	I-Tag Service ID	Specify the backbone service instance ID for the traffic.

Step5 On the backbone frame graphic, select **Data**, and then specify the settings that characterize the customer frame (illustrated in Figure 37 on page 128).

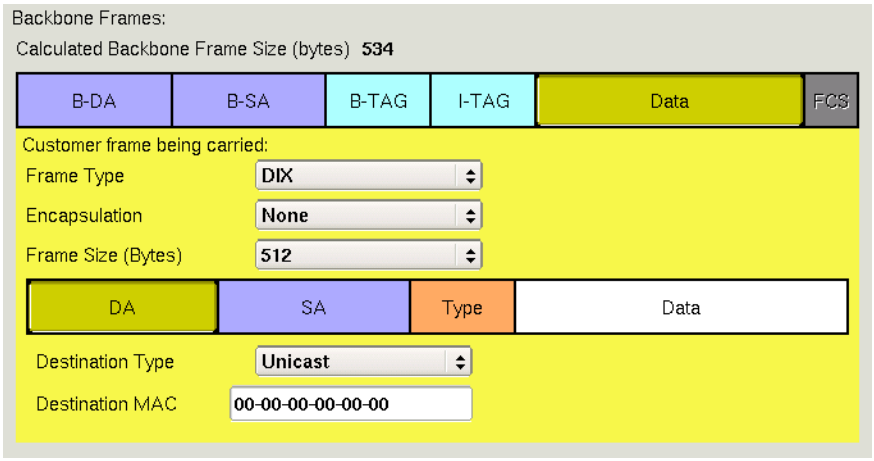


Figure 37 Customer Frame (MiM Traffic application)

Step6 On the customer frame graphic, select **Data**, and then specify one of the following for the Tx Payload:

– **Acterna.** To transmit frames that contain a sequence number and time stamp so that lost frames, round trip delay, and jitter can be calculated, select **Acterna**.

If you are measuring round trip delay on a 10 Gigabit circuit, in RTD Setup, indicate whether you want to measure delay with a high degree of precision, or a low degree of precision. In most instances, you should select **High Precision - Low Delay**.

NOTE: You must select an Acterna payload to measure round trip delay and count lost packets.

– **BERT.** To transmit frames with payloads filled with the BERT pattern you specify, select **BERT**, and then select a pattern.

- Various pseudo-random and Fixed patterns are available. The Pseudo-random patterns continue from one frame into the next. The fixed patterns restart each frame, such that the frame will always start with the beginning of the pattern.

- If you set the BERT Pattern to User Defined, in the User Pattern field, specify the 32 bit fixed pattern that will be repeated in the payload.

NOTE:

The Transport Module transmits the bytes in user defined patterns from left to right; the FST-2802 transmits the bytes in user defined patterns right to left.

For example, a user defined hexadecimal pattern of 12345678 populates the frame as: 12345678.Using the same hexadecimal pattern, the FST-2802 would populate the frame as 78563412.

Step7 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The transmitted frame settings are specified.

Specifying Ethernet filter settings for MiM traffic

Before transmitting or monitoring layer 2 traffic on a MiM trunk, you can specify settings that indicate the expected received payload and determine which backbone frames will pass through the receive filter and be counted in the test result categories for filtered layer 2 traffic. The settings may also impact other results.

If you want to observe results for the Customer Link (counts or statistics), ensure that the B-TAG and I-TAG filter settings, and the Customer filter settings match those carried in the analyzed traffic.



NOTE:

During layer 2 BER testing, incoming frames must pass the filter to be analyzed for a BERT pattern. Local loopback is also only performed on frames that pass the filter. Use the filter when analyzing BERT frames and non-test frames are present.

To specify Ethernet filter frame settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 3 on page 27 for a list of MiM applications.

Step2 Select the **Setup** soft key, and then select the **Ethernet Filter** tab.

Step3 Specify the settings required to filter received traffic for analysis:

Frame Label	Setting	Value
B-TAG	B-Tag VLAN ID Filter	If you don't want to filter traffic for a specific VLAN, select **Don't Care**; otherwise, select **Specify Value**.
	B-Tag VLAN ID	Enter the ID for the backbone VLAN used as the path to the destination. This setting only appears if B-Tag VLAN ID Filter is set to Specify Value.
	B-Tag Priority	Enter the priority code point (PCP) ID representing the type of service the filtered traffic is emulating, or select **Don't Care**.
	B-Tag DEI BIT	Indicate whether the filtered traffic is drop eligible by setting the DEI bit for the traffic, or select **Don't Care**.
I-TAG	I-Tag Priority	Enter the priority code point (PCP) ID representing the type of service the filtered traffic is emulating, or select **Don't Care**.
	I-Tag DEI Bit	Indicate whether the filtered traffic is drop eligible by setting the DEI bit for the traffic, or select **Don't Care**.
	I-Tag UCA Bit	Indicate whether the filtered traffic uses the customer address by setting the bit, or select **Don't Care**.
	I-Tag Service ID Filter	Specify the backbone service instance ID carried in the filtered traffic by selecting **Specify Value**, or select **Don't Care**.
	I-Tag Service ID	If you set the I-Tag Service ID Filter to **Specify Value**, specify the service instance ID carried in the filtered traffic. This setting only appears if I-Tag Service ID Filter is set to Specify Value.

Step4 Select the **Data** field on the illustration of the backbone frame, and then specify the following for the *customer frame*:

Setting	Value
Encapsulation	Select one of the following: – **None**. To analyze unencapsulated traffic, select **None**. – **VLAN**. To analyze VLAN tagged traffic, select **VLAN**, and then select the VLAN field on the illustration of the customer frame to specify the ID and priority. – **Q-in-Q**.To analyze Q-in-Q tagged traffic, select **Q-in-Q**, and then select the SVLAN field on the illustration of the customer frame to specify the SVLAN settings, and the VLAN field to specify the VLAN ID and priority. – **Don't Care**. To analyze all customer frames irrespective of encapsulation, select **Don't Care**. For details on the VLAN or Q-in-Q filter settings, refer to "Specifying Ethernet filter settings" on page 56.
Frame Type	Select one of the following: – **DIX** – **802.3**

Step5 Select the **Data** field on the illustration of the customer frame, and then do one of the following:

– If you want the module to monitor and analyze live Ethernet traffic by suppressing lost frames (LF) or BERT errors in their associated result counts and as triggers for LEDs during payload analysis, turn Payload Analysis **Off**.

– If you want to filter traffic for a particular pattern, turn Payload Analysis **On**, and then specify the BERT pattern.

Step6 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The received frame settings are specified.

Specifying OAM settings

You can position the instrument at various endpoints in a Maintenance Domain (MD) or Maintenance Association (MA) area to verify that no OAM trunk problems occur. For details, refer to "OAM service and link layer testing" on page 119

Specifying traffic load settings

Before transmitting layer 2 traffic over a MiM trunk, you can specify the type of traffic load the unit will transmit (Constant, Burst or Ramp). The settings vary depending on the type of load.

When configuring a load, you can specify the bandwidth of the transmitted traffic in 0.001% increments for 1 Gigabit or 10 Gigabit circuits, or 0.01% increments for 10/100/1000 Mbps electrical or 100 Mbps optical circuits.

For an overview of the available traffic loads, see "Specifying traffic load settings" on page 64.

Transmitting layer 2 MiM traffic

Before you transmit layer 2 traffic over a MiM trunk, you must specify:

– Interface settings (see “Specifying interface settings” on page 46).
– Frame characteristics of the transmitted traffic (see “Specifying Ethernet frame settings” on page 126).
– Frame characteristics used to filter received traffic (see “Specifying Ethernet filter settings for MiM traffic” on page 129).
– Traffic load settings (see “Specifying traffic load settings” on page 130).

After you specify the layer 2 settings, you are ready to transmit and analyze the traffic.

To transmit and analyze layer 2 traffic

Step1 If you haven’t already done so, use the Test Menu to select the MiM terminate test application for the interface you are testing.

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see “Specifying interface settings” on page 46).

Step3 Select the **Ethernet** tab to specify settings that define the frame characteristics of the transmitted traffic (see “Specifying Ethernet frame settings” on page 126).

Step4 Select the **Ethernet Filter** tab to specify settings that filter the received traffic based on specified frame characteristics (see “Specifying Ethernet filter settings for MiM traffic” on page 129).

Step5 Select the **Traffic** tab to specify the type of load the unit will transmit (see “Specifying traffic load settings” on page 130).

Step6 Press **Results** to return to the Main screen.

Step7 Connect the module to the circuit.

Step8 If you are testing an optical interface, select the **Laser** button.

Step9 Select **Start Traffic** to transmit traffic over the circuit.

Step10 Verify that the green Signal Present, Sync Acquired, Link Active, and PBB Frame Detect LEDs are illuminated.

Step11 At a minimum, observe the test results in the Summary Status result category.

You have analyzed layer 2 MiM traffic.

Inserting errors or pause frames

Action buttons on the Main screen allow you to insert errors and pause frames into the traffic stream. If you turn on a particular error insertion rate, the error insertion continues even after you restart a test or change the test configuration.

For detailed instructions on error and pause frame insertion, see “Inserting errors or pause frames” on page 105.

Measuring round trip delay and packet jitter

You can measure round trip delay and packet jitter by transmitting traffic carrying an Acterna payload. Frames with an Acterna payload provide time stamps, enabling the unit to calculate the delay and jitter. For instructions on looping back a unit, see Chapter 8 “Loop back Testing”.

For detailed instructions, see “Measuring round trip delay or packet jitter” on page 106.

Measuring service disruption time

You can use two units in an end-to-end configuration to measure the service disruption time resulting from a switch in service to a protect line. The traffic originating unit must transmit a constant rate of traffic to obtain accurate measurements.

For detailed instructions, see “Measuring service disruption time” on page 118.

Monitoring layer 2 MiM traffic

Use the MiM Traffic Monitor/Through application whenever you want to analyze received traffic. When you configure your test, you can specify settings that indicate the expected received payload and determine which frames will pass through the receive filter and be counted in the test result categories for filtered layer 2 traffic. The settings may also impact other results.



NOTE:

If you are testing from an optical interface, you must turn the laser on using the associated button to pass the signal through the unit’s transmitter.

For detailed instructions, see “Monitoring layer 2 traffic” on page 70.

Synchronous Ethernet testing

Synchronous Ethernet (Sync-E) is the ability to provide frequency distribution through an Ethernet port. Physical layer timing transport is required to guarantee frequency distribution to the extent necessary for encapsulated signals to meet network performance requirements. Although other methods may be used for this purpose, physical layer Sync-E provides the best technical option for guaranteed frequency accuracy and stability because it is impervious to the effects of traffic load. On a Sync-E network, each node in the network recovers the clock.

To test a signal containing Sync-E timing signals requires a Sync-E PIM and transceivers inserted into a Sync-E SFP PIM. If a non-Sync-E PIM is being used, it will not be able to receive or transmit Sync-E SSM signals.

To test Sync-E

Step1 If you haven’t already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 2 on page 26 through Table 3 on page 27 for a list of layer 2 and layer 3 applications. Table 12 on page 149 lists layer 4 applications.

Step2 Press the **Setup** soft key, and then select the **Interface** tab.

Step3 On the Physical Layer tab, check the box beside **Enable Synchronous Ethernet**. This specifies whether SSM messages are transmitted, decoded and have statistics collected about them.

- If it is desired to transmit SSM messages, **Enable** the SSM Tx.
- To define the rate of transmission (in PDUs/sec), select the Tx Rate from the drop-down box.
- Select whether the message type will be Informational or Event.
- Select the quality level (QL Value) of the clock - EEC2, EEC1 or DNU.

Step4 Select the **Results** soft button to return to the main screen and connect the instrument to the circuit.

Step5 Select the **Laser** button to turn on the laser.

Step6 Select **Start Traffic** to transmit traffic over the circuit.

Step7 Use the **Actions** buttons to add positive or negative frequency offset on the transmit line frequency. It should appear in the Rx Freq Deviation result on the far end, in the Interface category.

Step8 Observe the test results in the Signal category (in the Interface group) and the Sync Status Messages category (in the Ethernet group). For details, see “Interface results” on page 354 and “Sync Status Messages” on page 386 of Chapter 13 “Test Results”.

You have tested Synchronous Ethernet.

Transmitting and analyzing PTP/1588 traffic

You can use the instrument during turn-up or installation of PTP links or troubleshooting an active link. Features include the following:

– Verify that the link can support PTP
– Verify that the PTP Master is reachable and can be communicated with
– Verify that PTP timing messages are received
– Provide packet delay variation (PDV) measurements
– Load network background traffic stream simultaneously with PTP session to see effect network traffic has on PTP
– Connect an optional GPS as timing source
– Capability to measure master-to-slave and slave-to-master delay

About PTP

Due to growing wireless traffic volume, 3G and 4G networks are being deployed. In order to ensure accuracy and that inter-cell handoffs are manageable, every base transmission station in the network needs to be able to trace its frequency synchronization back to a primary reference clock. Without synchronization, the mobile devices lose lock which can adversely affect voice and data services or result in dropped calls.

Precision time protocol (PTP) is an industry-standard protocol that enables the precise transfer of frequency and time to synchronize clocks over packet-based Ethernet networks.It is based on IEEE 1588. The PTP protocol specifies master and slave clocks. It synchronizes the PTP local slave clock on each PTP network device with a PTP system Grandmaster clock. PTP distributes the timing at layer 2 or 4 using timestamps embedded within an Ethernet frame or IP/UDP packet; thus, PTP can be transported over native Ethernet or any transport that supports IP/UDP.

The Multiple Services Application Module can be configured as either a slave or a master unit in a PTP system. When configured as a master, the internal oscillator is used as the system clock to which all other units are synced. The measurement of the relative stability of this system is the Packet Delay Variation (PDV).

GPS as Time Source

In those systems where the PDV results indicate the need for greater stability, an option is available that utilizes a GPS Time of Day (ToD) and 1PPS signals to generate the timestamps and provide reference to a Grandmaster clock.

Connecting the GPS

The optional GPS receiver supplies the 1PPS and the ToD signal for use in generating PTP time-stamps. Different generations of these instruments utilize different connections for these signals. These connections are identical to those used for OWD (except for the CDMA connections). Refer to Figure 27 through Figure 35.

Before beginning the test, verify that the GPS receiver and instrument are synchronized and ready.

– Verify that the appropriate LEDs on the GPS receiver are flashing or steadily on (refer to the instructions included with the GPS receiver).
– Verify that the TOD Sync and 1PPS LEDs on the instrument are on.

To ensure maximum accuracy and stability, follow the guidelines regarding preparation time and hold-over stability included in the documentation shipped with the GPS receiver.

Configuring GPS as Source

After the GPS receiver is connected to the instrument, the instrument does not automatically switch to the GPS as time source. The instrument must be configured to use the GPS as the time source. If sync to the GPS is lost at any time though, the instrument will automatically switch to the internal oscillator as the PTP time source and an event will be recorded in the log.

To select GPS as time source

Step1 If you haven't already done so, use the Test Menu to select the PTP/1588 application for the interface you are testing. Refer to Table 5 on page 28 for a list of applications.

Step2 On the instrument, select the **Setup** soft key.

Step3 Select the **Interface** tab, and then on the **CDMA/GPS Receiver** tab, select the **Enable CDMA or GPS receiver** check box.

The GPS receiver has been selected as the time source.

Analyzing PTP traffic

You can use the instrument to send and receive traffic to troubleshoot a PTP link.

To transmit and analyze PTP traffic

Step1 If you haven't already done so, use the Test Menu to select the PTP/1588 application for the interface you are testing. Refer to Table 5 on page 28 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **PTP** tab.

Step3 Specify the settings:

Setting	Description
Mode	Specifies master or slave mode.

Setting	Description
Address Mode	In Slave mode, specifies the type of message: unicast or multicast. Multicast: PTP message (announce, sync and delay request) rates configured on Master. Unicast: PTP message rates configured on Slave.
Domain	Specifies the domain number that is using PTP. The domain is a logical grouping of clocks that synchronize to each other using PTP.
Sync Type	In Master mode, indicates that the synchronization type is two step.
Master IP Address	If testing layer 4 streams in slave mode, and the address mode is unicast, enter the IP destination address of the master.
Master MAC Address	If testing layer 2 streams in slave mode, and the address mode is unicast, enter the MAC destination address of the master.
Encapsulation	Specify the encapsulation: VLAN or None.
VLAN ID and Priority	If Encapsulation is set to VLAN, specify the ID and priority for the VLAN.
TOS Type	If testing layer 4 streams, specify the TOS type: TOS or DSCP.
TOS	If TOS type is TOS, specify the TOS code.
DSCP	If TOS type is DSCP, specify the DSCP code. DSCP values are shown as code points with their decimal values following in ( ). For example, EF(46).
Announce Rx Timeout	If in Slave mode, specify the amount of time that has to pass without receipt of an announce message to trigger a Timeout event.
Announce	Specify the announce message rate - the rate at which announce messages are transmitted. **NOTE:** When using multicast address mode, the announce rate must match for the Master and Slave. Although the Master controls the rate, the Slave must use the same rate, otherwise timeouts occur.
Sync	Specify the sync message rate - the rate at which sync messages are transmitted.
Delay Request	Specify the delay request message rate - the rate at which delay request messages are transmitted.
Query	If testing in the Slave mode and using unicast address mode, specifies the rate at which unicast messages are transmitted.
Lease Duration	If testing in the Slave mode and using unicast address mode, specifies the unicast lease duration, in seconds.
Priority 1	In Master mode, specify the priority 1 value - the priority is used in the execution of the best master clock algorithm.
Priority 2	In Master mode, specify the priority 2 value - the priority is used in the execution of the best master clock algorithm.
Class	Specify the clock class - the traceability of the time and frequency distributed by the grandmaster clock.
Time Source	Specify the source of time used by the grandmaster clock.
Clock Accuracy	Specify the estimated accuracy of the grandmaster clock.

Step4 Press **Results** to return to the Main screen.

If testing toward a unit that is in loopback, the stream bandwidth should be limited to 95% (on the “All Streams” tab, using “Configure Streams”).

Step5 Connect the instrument to the circuit.

Step6 If you are testing an optical interface, select the **Laser** button.

If testing layer4 streams, the Stream IP destinations must complete ARP successfully before PTP Session can be started.

Step7 Select the **Start PTP session** button.

Step8 Verify that the green Signal Present and Link Active LEDs are illuminated.

NOTE:

When running a PTP test, it is recommended you avoid CPU intensive actions such as launching another application, launching Wireshark, or saving a capture. These can cause a spike in PDV stats.

Step9 Observe the PTP Link Stats and PTP Link Counts.

NOTE:

The PTP session will be terminated if a loop down request is received. If you wish to save the test results, do so before looping down.

You have analyzed PTP traffic.

Discovering traffic using J-Profiler

If your instrument is optioned and configured to do so, you can use the J-Profiler application to automatically discover and monitor up to 128 streams of traffic that satisfy your profile criteria on 10/100/1000 electrical, 100M optical, and 1GigE optical circuits. After discovering the streams, you can sort them based on the bandwidth utilized by each stream to identify the top talkers for the discovered streams. If there are less than 128 streams present on the link, this represents the top talkers for the link. If there are more than 128 streams present on the link, this represents the top talkers for the streams satisfying your profile criteria.

When running the J-Profiler application, standard link and filtered results are provided in addition to the Traffic Profiler Streams results.

To discover traffic using J-Profiler

Step1 Use the Test Menu to select the J-Profiler test application for the interface you are testing.

Step2 Select the **Setup** soft key, and then select the Interface tab to specify settings that control the Ethernet interface (see “Specifying interface settings” on page 46).

Disable J-Profiler before changing IPv6 address modes. Failure to do so may cause the instrument to lock up.

Step3 If you want to discover streams sharing specific criteria (such as a particular VLAN, Source MAC address, or well-known TCP/UDP port), select the **Filter** tab, then specify the settings. For details, see:

- "Specifying Ethernet filter settings" on page 56
- "Specifying IPv4 filter settings" on page 85
- "Filtering received traffic using layer 4 criteria" on page 155

Only streams that satisfy the filter criteria will be discovered and displayed.

Step4 Select the **Profile** tab. The illustration in Figure 38 appears to guide you through the profile process:



Figure 38 J-Profiler illustration

Step5 Specify how the discovered (and optionally filtered) traffic will be displayed:

- VLAN ID. Both the VLAN ID and SVLAN ID will be considered. Traffic must contain at least one VLAN tag to be included in the profile.
- VLAN ID and Source MAC Address. Both VLAN IDs and the source MAC address will be considered. *The traffic does not need to carry a VLAN tag to be included in the profile*.
- VLAN ID, Source MAC and Destination MAC. Similar to VLAN ID and Source MAC Address, but also considers the destination MAC address. *Use this setting if you want to observe MAC-to-MAC conversations.*
- VLAN ID and Source IP Address. Both VLAN IDs and the source IP address will be considered. *The traffic does not need to carry a VLAN tag, but it must have a source IP address to be included in the profile.*
- VLAN ID and well-known (0-1023) TCP/UDP port. Both VLAN IDs and the TCP/UDP port number will be considered. *The traffic does not need to carry a VLAN tag, but it must be TCP or UPD traffic to or from a well known port to be included in the profile. Use this setting if you want to see which services are running (well-known ports typically identify services).*
- MPLS Labels with VLAN ID. Both MPLS labels and VLAN IDs will be considered. *The traffic does not need to carry a VLAN tag to be included in the profile*.
- PW (Pseudowire) Labels with VLAN ID. Both MPLS labels and PW labels along with VLAN IDs will be considered. *The traffic does not need to carry a VLAN tag to be included in the profile*.
- Source IP, Destination IP, Source Port and Destination Port. All four parameters will be considered. *These parameters form the two ends of a TCP or UDP conversation, so use this setting if you want to observe these conversations.*

Step6 Press **Results** to return to the Main screen.

Step7 Connect the module to the circuit.

Step8 If you are testing an optical interface, select the **Laser** button.

Step9 Select **Start Traffic** to transmit traffic over the circuit.

Step10 At a minimum, verify that the green Signal Present, Sync Acquired, Link Active, and Frame Detect LEDs are illuminated.

Step11 At a minimum, observe the test results in the Traffic Profile group, in the Streams category. For details, see “J-Profiler results” on page 395 of Chapter 13 “Test Results”.

You have discovered traffic using J-Profiler.

5

Wander Testing

This chapter provides step-by-step instructions for measuring wander on 1GigE Optical SyncE networks using the instrument. Topics discussed in this chapter include the following:

– “About wander testing” on page 140
– “Measuring and analyzing wander” on page 140

About wander testing

If your MSAMv2 is configured and optioned to do so, you can use it to measure wander on a 1GigE Optical SyncE interface. (both the SyncE and Wander options must be installed). For details on the device and interface standards for measuring jitter and wander on Ethernet interfaces, refer to *ITU-T Recommendations O.174*.

NOTE

Due to intense resource requirements, the Wander test must be run exclusively. No other test may be run simultaneously on a unit making wander measurements.

Wander testing is only applicable to 8000 UIMv2 and MSAMv2 or higher.

The wander option allows you to analyze system wander performance.

NOTE:

The MSAM has a maximum wander test duration of 48 days 23 hours 59 minutes and 56 seconds, but may be limited by file system storage capacity (actual time available may be less). When running a test, you can observe the remaining test time in the Time category of the Summary result group or in the Wander category of the Interface result group.

For information about jitter and wander principles and specifications, refer to the appendix “Principles of Jitter and Wander Testing” in the *PDH, SONET, SDH, NextGen, and OTN Testing Manual*.

Features and capabilities

The wander measurement includes the following:

– Allows you to test and analyze the wander results in a graphical manner.
– Export the wander TIE result to be analyzed on a remote PC using the O.172 MTIE/TDEV Offline Analysis software shipped with your unit. For details, see “Saving and exporting wander measurement data” on page 145.

Accessing wander test results

When you configure your unit to measure wander, measurement results are available in the Interface result group.

Measuring and analyzing wander

If you purchased the wander testing option, you can measure Time Interval Error (TIE) and calculate MTIE/TDEV (Maximum Time Interval Error/Time Deviation) to evaluate the condition of your network elements.

NOTE:

The time it takes to update the TIE data or calculate MTIE/TDEV depends on the amount of data collected.

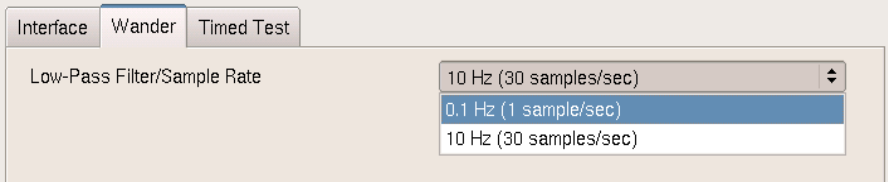
Measuring TIE and calculating MTIE

Measuring TIE and calculating MTIE involves specifying the settings for the test interface you selected and the Tx and Rx parameters. After the test starts, you can observe the TIE and MTIE results in the Wander category.

To measure TIE and MTIE

Step1 Using the Test Menu, select the **Ethernet>1GigE Optical>SyncE Wander** test application.

Step2 Select the **Setup** soft key, and then select the **Wander** tab.



Step3 Specify the wander sample rate.

Step4 Select the **Results** soft key to return to the Main screen.

Step5 Connect the a cable from the appropriate TX connector to the network's Rx access connector.

Step6 Connect the reference signal to the appropriate input.

Step7 Select the **Laser** button.

The button label becomes Laser On.

Step8 Verify the LEDs.

– Verify that the Signal Present, Sync Acquired, and Link Active LEDs are green.

– Verify that the Wander Reference Present is green.

Step9 Select **Restart**.

Step10 Run the test for an appropriate length of time. To ensure accuracy of your results, let the test run for at least one minute.

Step11 To view the wander results, set one of the result windows to display the Summary group, set another results window to display the Interface group, and then select the Wander category.

To view the wander results in a graphical format, select the Wander Graph category. For details, see "Wander Interface results" on page 396.

TIE and MTIE results are measured.

SyncE Reference Timing Wander

If your MSAMv2 is configured and optioned to do so, you can use it to measure wander of a Synchronous Ethernet timing signal to a stable reference signal

To measure SyncE wander to timing reference signal

Step1 Using the Test Menu, select the wander application for the signal you are testing.

Step2 Select the **Setup** soft key.

Step3 On the Wander tab specify the desired **Low Pass Filter/Sample Rate** from the drop down box.Select the arrows to the right of the Low-Pass Filter field, and then select the desired Rx filter value.

The filter you specify automatically determines the sampling rate for the wander measurement.

Step4 On the Timed Test tab define the starting time and length of test parameters.

Step5 Select the **Results** soft key.

Step6 Check that the reference signal is connected to the appropriate connector on the unit as detailed inTable 11 on page 142. If the unit is not properly configured to accept a particular type of reference signal, a message will be displayed indicating the reference signal is not supported.

Table 11 Reference Signal Input Connectors

External Reference Signal	Reference Input Connector
BITS[a]	SMA
SETS[a]	SMA
2.048MHz	SMA
10.0 MHz	SMA

a. Measurement against BITS or SETS requires CIB rev 008 or greater. To view the revisions of internal components, use the System Info menu.

Step7 Select **Restart**.

Step8 Run the test for an appropriate length of time. To ensure accuracy of your results, let the test run for at least one minute.

Step9 To view the wander results, set one of the result windows to display the Summary group, set another results window to display the Interface group, and then select the Wander category.

To view the wander results in a graphical format, select the Wander Graph category.

SyncE TIE and MTIE results are measured.

Analyzing wander

After you have accumulated some TIE data samples, the MSAM can do more detailed MTIE and TDEV calculations on it using the On-board Wander Analysis tool. This provides much more detail than the results available in the Interface/Wander category.

Step1 To analyze wander, follow step 1 through step 11 of “Measuring TIE and calculating MTIE” or step 1 through step 9 of “SyncE Reference Timing Wander”.

Step2 Select the **Wander Analysis** soft key.

The graphical wander analysis screen appears with the TIE tab selected.

NOTE:

– You can run the on-board Wander Analysis while the test is in progress, however, if you modify the sample rate or restart the test, the wander data collected previously will be cleared. If you want to preserve the wander data for the previous measurement, save the data before restarting a test. Note: the saved data cannot be loaded into the on-board Wander Analysis tool; it calculates MTIE and TDEV on all the data accumulated so far.

– Wander analysis is restricted to the first 8.64 million samples. If your measurement contains more samples, you must export the wander data for offline analysis.

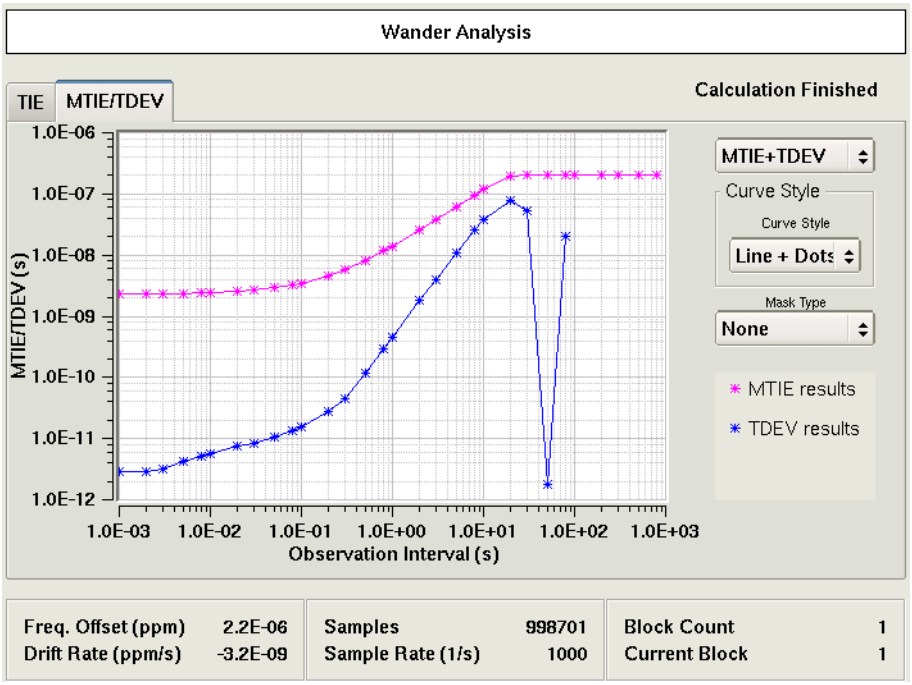
– Wander analysis is a memory intensive operation. Therefore, you can only process wander data while running a single application.

For detailed information about saving and exporting wander data, see “Saving and exporting wander measurement data” on page 145.

Step3 Select the **Update TIE Data** soft key.

This refreshes the data in the Wander Analysis screen. All of the TIE samples accumulated so far (including those gathered since the tool itself was launched) are redrawn, and then MTIE and TDEV are recalculated.

The TIE graph appears. The Wander Analyzer automatically displays the last block of continuous valid data.



Step4 To observe another block of data, select the Current Block field, type the block number, and then select **OK**.

The data block you specified appears.

A block of TIE data is a contiguous subset of all TIE samples that is not interrupted by any alarms. For Wander measurements, TIE values are sampled at a constant rate. If an alarm occurs (e.g. LOS), the receiver is not able to produce meaningful TIE values and stops producing TIE entries until it is able to recover. These alarms separate the whole measurement into sections, or “blocks”.

Step5 If you want to observe the frequency offset curve, clear the **Remove Offset** checkbox.

Step6 To select the data curve to observe, under Curve Selection, do one of the following:

– To observe both TIE and frequency offset data curves, select **Both Curves**.

– To observe only the frequency offset data curve, select **Offs.rem.only**.

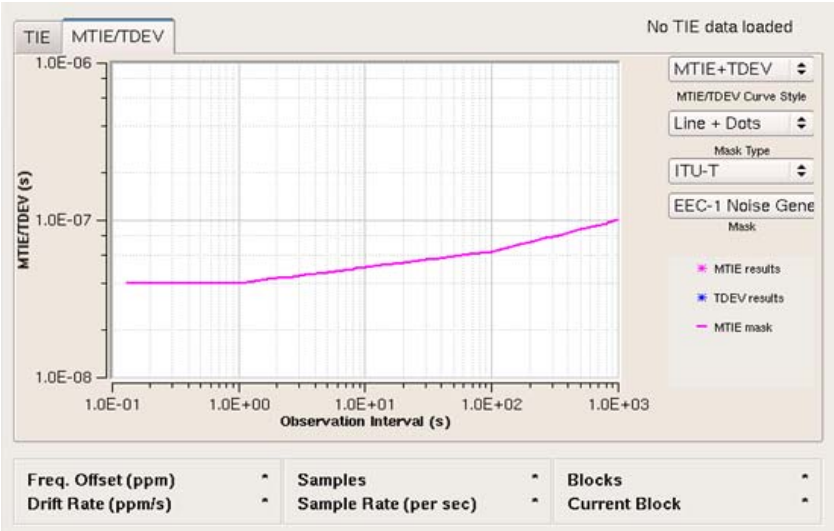
Step7 To refresh the graph, select the **Update TIE Data** soft key again.

Step8 To observe the MTIE/TDEV result graph, select the MTIE/TDEV tab.

The MTIE/TDEV graph screen appears.

Step9 Select **Calculate MTIE/TDEV** to start calculating MTIE and TDEV results.

The MTIE/TDEV graphs appear.



Step10 To customize the graph, do the following:

a To select the data curves you want to observe, use the first field to select **MTIE only**, **TDEV only**, or **MTIE+TDEV**.

b To select the curve style, select the arrows to the right of the Curve Style field, and then select **Line+Dots**, or **Dots only**.

Step11 If you want to select a mask to compare the data against, do the following:

a In the Mask Type field, specify a mask type.

b In the Mask field, specify a mask to compare the data to.

The mask curve appears on the result graph.

If you do not want to compare the data against a mask, in the Mask field, select **None**.

Step12 Do one of the following:

– To stop calculating MTIE/TDEV before the calculation is complete, select the **Stop Calculation** soft key.

– To refresh the graph, select **Calculate MTIE/TDEV** again.

– To return to the Main screen, select the **Results** soft key.

– To stop wander analysis and return to the Main screen, select the **Close Analysis** soft key.

NOTE:

Selecting the Close Analysis soft key stops analyzing the data and clears test results. This will discard all MTIE and TDEV results calculated inside the Analysis tool. It will not discard the real-time MTIE results displayed in the Interface/Wander category. To return to the Main screen without ending the current analysis, use the **Results** soft key.

Saving and exporting wander measurement data

You can save the TIE result data to a .hrd file or .chrd (compressed and encrypted .hrd file) on the base unit's hard drive, then export the saved file to a USB memory key, and then do further analysis of MTIE and TDEV by loading the file on a remote PC using an offline analysis tool, such as the PC-based *Wander Analysis* application.

NOTE:

Restarting a test clears the wander history data. If you want to preserve the wander data for the current measurement, you must export the data before restarting a test.

To save the TIE data

Step1 Select the **Save TIE Data** soft key.

The wander data is saved into a .hrd or .chrd file in the following folder on your unit:

`../acterna/user/disk/bert/reports`

The file name is automatically assigned with a `TIE_` prefix followed by date, time, test mode, and interface information as shown in the following example:

`TIE_2007-08-16T15.59.19_TermDs1WanderTieEvalMsec.hrd`

The TIE data is saved.

NOTE:

The offline analysis tool *TIE - MTIE/TDEV Analyzer* can analyze .hrd files only, however, the *Wander Analysis* tool can analyze either .hrd or .chrd files.

If you have the *TIE - MTIE/TDEV Analyzer* tool but would like the *Wander Analysis* tool, contact customer service. The ordering number is
BN 3061/95.98.

If you have the *Wander Analysis* tool, version 3.0.0 or before, you can upgrade to the latest version for free, using the instructions provided in the user manual that came with the analysis tool.

To export the TIE data to a USB memory key

Step1 Insert a USB memory key into one of the two slots provided on the top panel of the base unit.

Step2 Select the **Export TIE Data** soft key.

The Wander Data Files screen appears, listing the wander data files in:

`../acterna/user/disk/bert/reports`

Step3 Select the wander data file you want to export, and then press the **Export to USB** soft key.

The File Export dialog box appears, indicating that the unit is copying the selected report file to the USB memory key.

The TIE data is exported. If desired, it can now can be loaded into the PC-based Wander Analysis Tool.

6

TCP/UDP Testing

This chapter provides step-by-step instructions for testing TCP/UDP service. Topics discussed in this chapter include the following:

– “About TCP/UDP testing” on page 148
– “Specifying layer 2 and layer 3 settings” on page 152
– “Specifying layer 4 settings” on page 152
– “Transmitting layer 4 traffic” on page 157
– “Inserting errors or pause frames” on page 157
– “Loopback testing” on page 157
– “Running TCP Host or Wirespeed applications” on page 158
– “TrueSpeed” on page 164

About TCP/UDP testing

If your instrument is configured and optioned to do so, you can use it to verify layer 4 performance by transmitting and analyze TCP or UDP traffic, verifying that routers are prioritizing traffic for various ports properly, and verifying that the bandwidth allocated to a customer per their Service Level Agreement is available. Figure 39 illustrates the Main screen when running a Layer 4 TCP/UDP application.

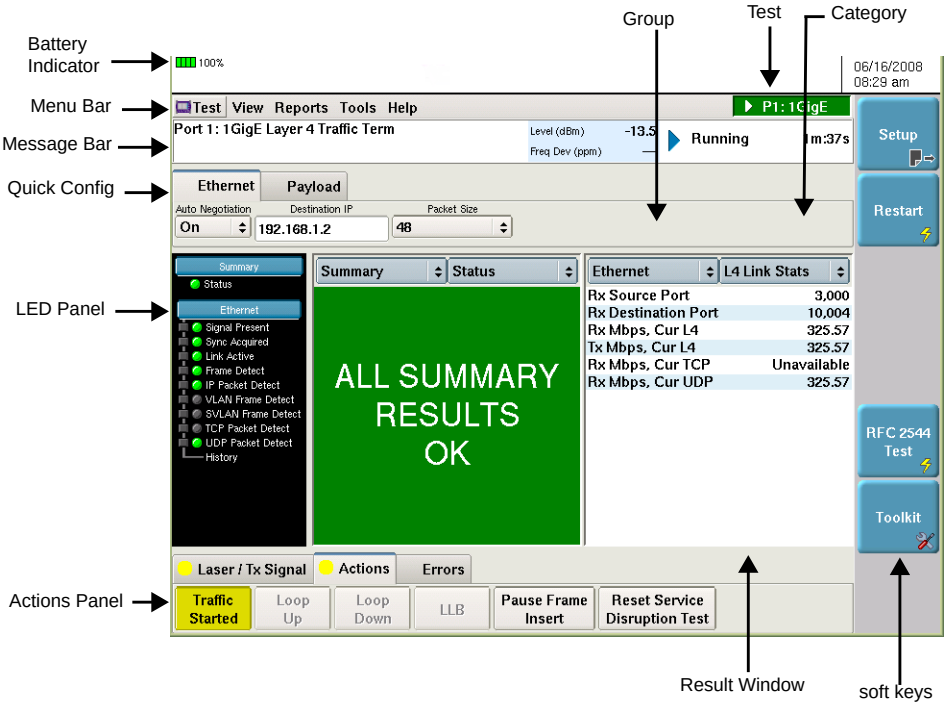


Figure 39 Main screen, Layer 4 Traffic application

Features and capabilities

Features and capabilities of the instrument include the following when testing TCP/UDP:

- Performance measurements—Layer 4 bandwidth, data loss, out of sequence, jitter, and latency measurements are available when evaluating layer 4 performance.
- Stateless firewall verification—You can configure and transmit TCP and UDP traffic destined for a particular port, and then verify that the traffic successfully passes through a stateless firewall.
- TCP connection support—The instrument can establish a TCP connection, enabling you to verify that traffic destined for a particular port can pass through stateful devices on the network.
- Multiple stream testing—You can transmit and analyze up to ten streams of layer 4 traffic, with each stream depicting a particular type of traffic. After transmitting the streams, you can analyze each stream to verify that network routing and switching devices are handling the traffic properly (based on each stream's priority). For details, see "Specifying layer 4 stream settings" on page 179.
- Layer 4 Toolkit—When running multiple streams applications, a variety of scripts have been provided in the Layer 4 Toolkit which allow you to determine the ideal window size, and measure throughput and latency for a particular connection.

– Packet capture and analysis—If your instrument is configured and optioned to do so, you can use it to capture transmitted and received data, save it on the instrument or to an external USB key, and then either send the data to another technician for analysis, or analyze it yourself using the Wireshark® protocol analyzer (provided on the instrument). For details, see "Capturing packets for analysis" on page 93.
– IPv6 support—If you purchased the IPv6 Traffic option, you can transmit and analyze IPv6 traffic using the terminate and monitor/thru applications. For details, see "Configuring IPv4 and IPv6 tests" on page 32.
– TCP Wirespeed throughput analysis—If your instrument is configured and optioned to do so, you can use it to verify that your network meets or exceeds the throughput specified in service level agreements at the TCP layer, and optimize layer 4 throughput by testing using a variety of window sizes. For details, see "Running the TCP Wirespeed application" on page 162.

Understanding the graphical user interface

When you configure your module for testing, graphical displays of TCP packets or UDP datagrams are provided on the setup tabs for the application you selected. You can specify characteristics for transmitted and filtered traffic by selecting the corresponding field on the graphic, and then entering or selecting a value. Colored fields can be edited; fields in gray can not be modified.

Figure 40 illustrates the TCP packet details for a layer 4 traffic test.

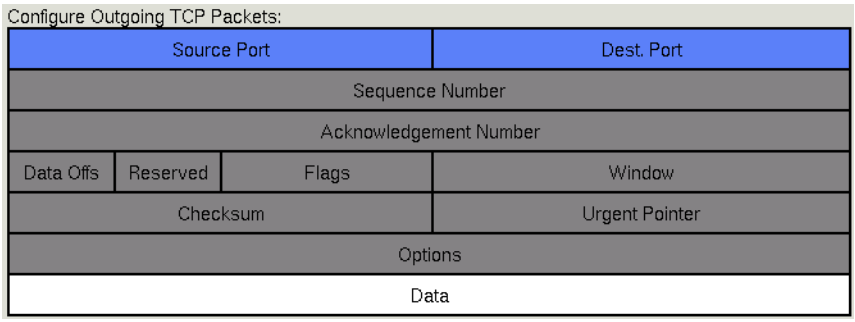


Figure 40 TCP Packet Details

For details on specifying layer 4 traffic characteristics, see "Specifying TCP/UDP settings for transmitted traffic" on page 153.

TCP/UDP test applications

If your instrument is configured and optioned to do so, the applications listed in Table 12 are supported.

Table 12 TCP and UDP applications

Circuit	Application	Test Mode[a]
10/100/1000	Layer 4 Traffic	Terminate Loopback
	Layer 4 Multiple Streams	Terminate Loopback
	Layer 4 TCP Wirespeed[b]	Terminate

Table 12 TCP and UDP applications (Continued)

Circuit	Application	Test Mode[a]
100M Optical	Layer 4 Traffic	Terminate Loopback
	Layer 4 Multiple Streams	Terminate Loopback
1GigE Optical	Layer 4 Traffic	Terminate Loopback
	Layer 4 Multiple Streams	Terminate Loopback
	Layer 4 TCP Wirespeed[b]	Terminate
10GigE LAN	Layer 4 Traffic	Terminate
	Layer 4 Multiple Streams	Terminate
	Layer 4 TCP Wirespeed[b]	Terminate

a. When running loopback tests, if both units are capable of transmitting traffic, select a Terminate mode application for each unit. If the loopback unit cannot transmit traffic, place it in Loopback mode. Loopback mode *does not appear* if your unit is capable of transmitting traffic.

b. IPv4 traffic only.

In addition to the single stream applications, you can also transmit and analyze up to ten streams of layer 4 traffic using the Layer 4 Multiple Streams application, or four streams using the Layer 4 TCP Wirespeed application. When running the Multiple Streams or Wirespeed applications, you can configure your instrument to emulate a TCP client or server, and then use the TCP Host to initiate a stateful TCP session with another device. For details, see "Specifying layer 4 stream settings" on page 179 and "Running the TCP Host script" on page 187 of Chapter 7 "Triple Play and Multiple Streams Testing".

Understanding the ATP Listen IP and Port

Many applications (such as delay measurements, out of sequence counts, lost frames counts, and packet jitter measurements) and multiple-stream tests must be performed using traffic that carries an Acterna Test Packet (ATP) payload. Each of these packets has a time stamp and a unique sequence number which are used to calculate a variety of test results.

The instrument uses the ATP Listen IP Address and ATP Listen Port to determine whether received layer 4 traffic carries an ATP payload; therefore, it is essential that you specify the correct ATP Listen IP Address and ATP Listen Port on the receiving unit when you configure tests that require an ATP payload.

Figure 41 illustrates the settings required to analyze layer 4 traffic carrying an Acterna payload when testing end-to-end.

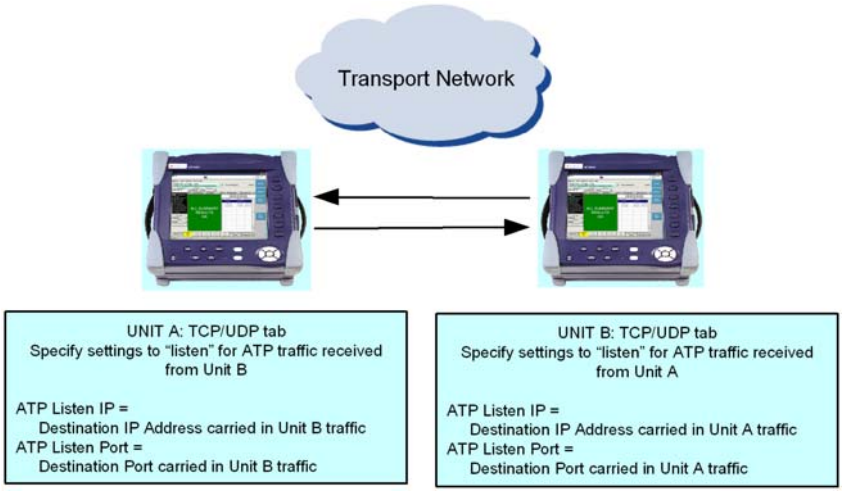


Figure 41 ATP Listen Scenario: End-to-End testing

When initiating a loop back from the local unit (using the Loop Up command), no ATP listen settings need to be specified for either unit (see Figure 42).

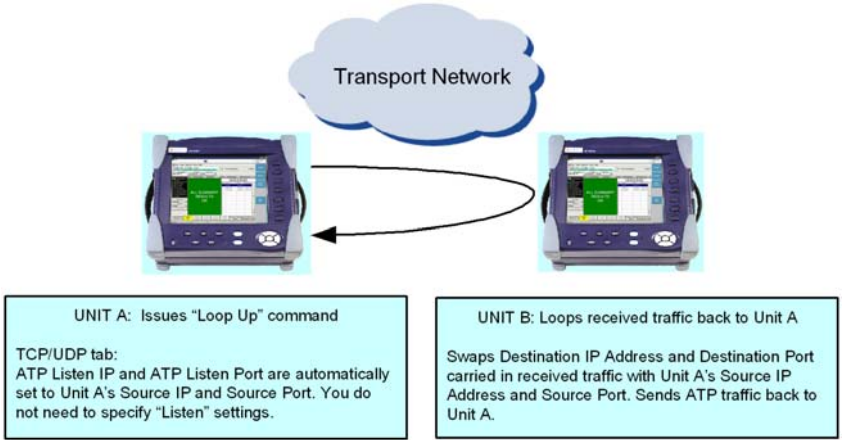


Figure 42 ATP Listen Scenario: Loop Up initiated from Unit A

Figure 43 illustrates the settings required for Unit A when traffic is looped back from the Unit B using the LLB action.

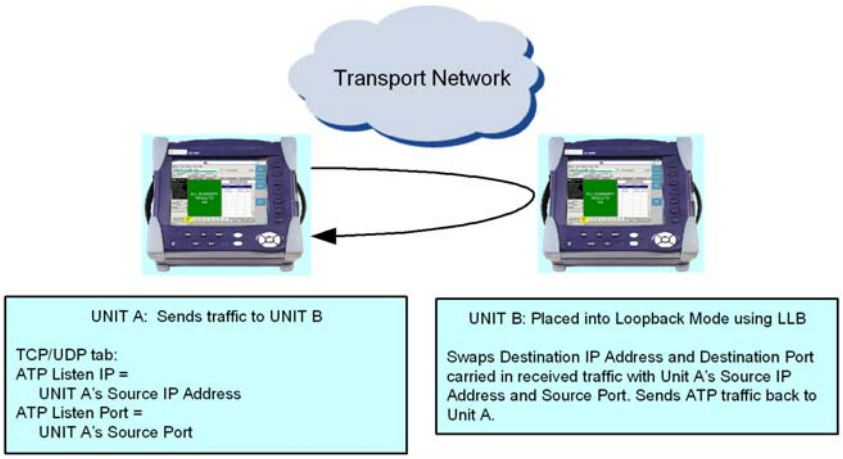


Figure 43 ATP Listen Scenario: LLB initiated from Unit B

For details, see "Specifying TCP/UDP settings for transmitted traffic" on page 153.

Specifying layer 2 and layer 3 settings

Before you transmit layer 4 traffic, you must first initialize the link, and specify the appropriate layer 2 and layer 3 settings for the traffic, such as the frame type, frame encapsulation, time to live, and type of service. After you initialize the link and specify the layer 2 and layer 3 settings, you then specify the required layer 4 settings before transmitting the traffic over the circuit.

For details on link initialization, see "Specifying interface settings" on page 46. For details on specifying layer 2 and layer 3 settings, see "Layer 2 testing" on page 46 and "Layer 3 testing" on page 78.

Specifying layer 4 settings

After initializing the link and specifying layer 2 and layer 3 settings, you specify the layer 4 settings before transmitting traffic over the circuit. Step-by-step instructions are provided in this section for the following:

- "Specifying TCP/UDP settings for transmitted traffic" on page 153
- "Configuring the traffic load" on page 154
- "Specifying the frame or packet length for transmitted traffic" on page 154
- "Filtering received traffic using layer 2 or layer 3 criteria" on page 155
- "Filtering received traffic using layer 4 criteria" on page 155

NOTE:

If during the course of testing you change the frame or packet length (or settings that impact the calculated length) while the unit is already transmitting traffic, the unit resets your test results, but some residual frames or packets of the old length may be counted because they are already in the traffic stream.

Well known ports

A port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports, known as well known ports, have numbers that are pre-assigned to them by the IANA (as specified in RFC 1700). Port numbers can range from 0 to 65535, but only ports numbers 0 through 1024 are reserved for privileged services and designated as *well-known ports*. This list of well-known port numbers specifies the port used by the server process as its contact port.

When configuring layer 4 traffic, you can select from a list of well known ports, or you can specify your own user-defined port.

Specifying TCP/UDP settings for transmitted traffic

Before transmitting layer 4 traffic you must specify the traffic mode, source and destination port numbers, and the type of payload carried.

Port 0 (zero) is reserved by TCP/UDP for networking; therefore, it is not available when you configure your traffic.

The following port numbers are also reserved, and should not be used during testing.

- 53
- 68
- 111
- 1022
- 1023
- 3000
- 3001
- 5353
- 8192

If DHCP is enabled in the near-end unit, a far-end unit should not send UDP traffic to port 68 for IPv4 and 546 for IPv6. Such UDP traffic may cause the near-end unit to lock up.

To specify the TCP/UDP settings for transmitted traffic

Step1 Using the Test Menu, select the Layer 4 Traffic application for the circuit you are testing (refer to Table 12 on page 149 for a list of applications).

Step2 Select the **Setup** soft key, and then select the TCP/UDP tab.

Step3 Specify the following settings:

Setting	Parameter
Traffic Mode	Indicate whether you want to transmit TCP or UDP traffic.

Setting	Parameter
ATP Listen IP Type	– To analyze ATP traffic carrying the source IP address of your unit as the destination address, select **Auto Obtained**. – To analyze ATP traffic carrying a different destination address (for example, a multicast address), select **User Defined**. Refer to "Understanding the ATP Listen IP and Port" on page 150 for illustrations explaining the ATP Listen settings for end-to-end and loop back tests.
ATP Listen IP Address (if ATP Listen IP Type is User Defined)	Specify the destination IP address carried in the ATP traffic that you want to analyze. **NOTE:** If your unit has been looped up by another unit, the ATP Listen IP Address will automatically be populated for you.
Listen Port Service Type	– To analyze ATP traffic with a specific service type, select the type. The ATP Listen Port will automatically be assigned for you. – To analyze ATP traffic with a service type that is not pre-defined, select **User Defined**.
ATP Listen Port (if Listen Port Service Type is User Defined)	Specify the port number carried in the ATP traffic that you want to analyze.
Source Port	Select a a pre-defined port number, or select User Defined to enter a different number.
Destination Port	Select a a pre-defined port number, or select User Defined to enter a different number.
Data	Select one of the following: – **Acterna.** To transmit packets that contain a sequence number and time stamp so that lost packets, round trip delay, and jitter can be calculated, select Acterna, and then specify the byte value that will be used to fill the rest of the payload using a 1 byte hexadecimal format. – **Fill Byte.** To transmit packets with payloads populated with a specific pattern of bytes, select Fill Byte, and then specify the byte value using a 1 byte hexadecimal format.

Step4 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The layer 4 settings are specified for transmitted traffic.

Configuring the traffic load

Before transmitting TCP or UDP traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty or Ramp) in 0.001% increments, beginning at 0.001%. For details on configuring a traffic load, see "Specifying traffic load settings" on page 64 of Chapter 4 "Ethernet and IP Testing".

Specifying the frame or packet length for transmitted traffic

Before transmitting TCP or UDP traffic, you must indicate the frame or packet length for each transmitted packet or datagram.

To specify the frame or packet length

Step1 If you haven't already done so, use the Test Menu to select the Layer 4 Traffic application for the circuit you are testing (refer to Table 12 on page 149 for a list of applications).

Step2 Select the **Setup** soft key, and then do the following:

a Go to the Ethernet tab.

b If you are specifying the length as a frame size, set the Length Type to **Frame Size**, and then select or specify the size.

The automatically calculated packet length appears to the right of the Length Type setting.

c If you are specifying the length as a packet length, set the Length Type to **Packet Length**, and then select or specify the size.

The automatically calculated frame size appears to the right of the Length Type setting.

The frame or packet length is specified.

Filtering received traffic using layer 2 or layer 3 criteria

If you want to filter received traffic using layer 2 or layer 3 criteria, set the Filter Mode to detailed on the Filters tab, select Ethernet or IP on the left pane, and then specify the criteria. For details, see "Specifying Ethernet filter settings" on page 56, "Specifying IPv4 filter settings" on page 85, or "Specifying IPv6 filter settings" on page 87 of Chapter 4 "Ethernet and IP Testing".

IPv6 traffic is not supported when running the TCP Wirespeed application.

Filtering received traffic using layer 4 criteria

You can specify settings that determine which packets will pass through the layer 4 (TCP/UDP) receive filter and be analyzed and reported in the test result categories, or looped back to another unit. Traffic that does not pass filter criteria is not reported or looped back.



FILTER TIPS:

– If you want to analyze all received traffic, Filter Mode is set to **Basic**.

– If you want to analyze only layer 4 traffic, be certain to set the Filter Mode to **Detailed**, and then **Enable** the TCP/UDP filter.

To specify TCP/UDP filter criteria

Step1 If you haven't already done so, use the Test Menu to select the Layer 4 application for the circuit you are testing (refer to Table 12 on page 149 for a list of applications).

Step2 Select the **Setup** soft key, then select the Filters tab.

Step3 In the panel on the left side of the tab, select **Basic**, then set the Filter Mode to **Detailed**.

Step4 Specify the Ethernet and the IP filter settings (see "Specifying Ethernet filter settings" on page 56, "Specifying IPv4 filter settings" on page 85, or "Specifying IPv6 filter settings" on page 87 of Chapter 4 "Ethernet and IP Testing").

Step5 To specify layer 4 filter settings, in the panel on the left side of the tab, select TCP/UDP, and then specify values for the following settings:

Setting	Parameter
Filter Enable	– If you want to filter received traffic using layer 4 criteria, select **Enable**. If you want to analyze only layer 4 traffic, you must enable the filter. – If you do not want to filter received traffic using layer 4 criteria, select **Disable**.
Protocol (if filter is Enabled)	– To analyze TCP traffic, select **TCP**. – To analyze UDP traffic, select **UDP**. – To analyze all layer 4 traffic, select **Don't Care**.
Port Filter	– **Single Direction.** To pass through the filter, traffic must satisfy the source and destination port criteria you specified for the filter to be reflected in the L4 Filter Counts and L4 Filter Stats result categories. – **Either Direction.** The filter will not care which direction the traffic is coming from; therefore, the source port carried in the filtered traffic can be the source port of the near-end instrument or port, or the source port of the far end instrument or port. Traffic from either source will be reflected in the L4 Filter Counts and L4 Filter Stats result categories.

Step6 On the graphic of the TCP/UDP packet, specify the following:

Setting	Parameter
Source Port (if filter is Enabled)	Two filters are available. If you define a single filter, traffic must match the criteria in the filter. If you define both filters, traffic must match the criteria for *either* filter. – Under **Filter 1**, if you want to filter traffic for a particular service type or source port, select the box to the left of **Source Service Type.** – To analyze traffic originating from one of the pre-defined specific service types, select the type. The port number is assigned automatically for you. – To analyze traffic originating from a different port, select **User Defined**, then specify the port number. – If you would like to define a second filter, specify the settings for **Filter 2**.
Destination Port (if filter is Enabled)	Two filters are available. If you define a single filter, traffic must match the criteria in the filter. If you define both filters, traffic must match the criteria for *either* filter. – Under **Filter 1**, if you want to filter traffic for a particular service type or destination port, select the box to the left of **Destination Service Type**. – To analyze traffic destined for one of the pre-defined specific service types, select the type. The port number is assigned automatically for you. – To analyze traffic destined for a different port, select **User Defined**, then specify the port number. – If you would like to define a second filter, specify the settings for **Filter 2**.

Step7 If you want to specify received payload settings, see “Filtering traffic using payload criteria” on page 63.

Step8 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The unit is configured to analyze received traffic satisfying the layer 4 filter criteria.

Transmitting layer 4 traffic

After you configure the layer 4 settings, you are ready to transmit traffic over the circuit.

To transmit layer 4 traffic

Step1 If you haven’t already done so, use the Test Menu to select the Layer 4 Traffic application for the circuit you are testing (refer to Table 12 on page 149 for a list of applications).

Step2 Specify the settings required to initialize the link (see “Specifying interface settings” on page 46).

Step3 Configure the instrument as appropriate for your test (see the appropriate procedures below):

- “Specifying Ethernet frame settings” on page 49
- “Specifying Ethernet filter settings” on page 56
- “Specifying traffic load settings” on page 64
- “Specifying transmitted IPv4 packet settings” on page 83
- “Specifying IPv4 filter settings” on page 85
- “Specifying TCP/UDP settings for transmitted traffic” on page 153
- “Specifying the frame or packet length for transmitted traffic” on page 154
- “Filtering received traffic using layer 4 criteria” on page 155

Step4 Press **Results** to return to the Main screen.

Step5 Select the **Action** tab, and then select **Start Traffic** (if you configured a constant or bursty load), or **Start Ramp** (if you configured a ramped traffic load).

The instrument transmits traffic over the circuit.

Inserting errors or pause frames

You can use the instrument to insert errors (such as TCP/UDP checksum errors) or pause frames into layer 4 traffic when you perform end-to-end and loop back tests. For details on error and pause frame insertion, see “Inserting errors or pause frames” on page 105.

Loopback testing

Loop back testing allows you to transmit traffic from one JDSU Ethernet test set, and then loop the traffic back through a second unit on the far end of a circuit. For details, refer to Chapter 8 “Loop back Testing”.

Running TCP Host or Wirespeed applications

If your instrument is configured and optioned to do so, the TCP Host application allows you to establish a TCP connection to a peer, and then measure layer 4 (TCP) throughput to demonstrate that poor application performance is not due to IP network issues. You can also determine the window size and latency associated with the connection. The TCP Host application is available when testing using a Transport Module or MSAM.

When testing using an MSAM, you can also use the TCP Wirespeed application to verify that your network meets or exceeds the layer 4 TCP throughput specified in customer's service level agreements for 10 Mbps through 10 Gbps circuits. Using TCP Wirespeed, you can demonstrate that problems are occurring due to customer applications such as file downloads, email, or internet access, rather than poor throughput on your network.

Unlike PC-based test solutions such as Iperf, the TCP Wirespeed application resides on your MSAM, eliminating many of the limitations and inaccuracies associated with poor PC performance. The application is not available on the Transport Module.

When configuring these applications, you can indicate whether you want the instrument to report throughput in kilobits, megabits, kilobytes, or megabytes per second. When configuring the TCP Host application, you can also specify the interval at which the instrument is to refresh reported test results.

IMPORTANT:

The TCP Host and TCP Wirespeed applications are resource intensive applications. To ensure optimal performance, be certain to configure one instrument as the client, and the other as a server (if you are using a second instrument rather than an Iperf server). Dual port testing is not recommended.

NOTE: Interrupted Connections

If a TCP connection is lost unexpectedly (or intentionally, for example, because someone brings the link down), the connection may not be restored automatically. This is expected behavior because there is no way to ensure that the server will become active before the client.

Changing settings during the test

When running the TCP Host and TCP Wirespeed applications, the instrument locks the Setup soft key and does not allow you to change application settings. This is to prevent you from mistakenly bringing the connection or connections down. If TCP connections come down when testing, there is no way to ensure that the server will become active before the client, and as a result, the instrument might not be able to restore the connection automatically.

Streams pipe: multiple TCP streams

When running the TCP Host or TCP Wirespeed application, you can use the Streams Pipe soft key to specify the load unit, and to access the Load Distribution dialog box. The Load Distribution dialog box is used to enable the background streams that you want to transmit, and to specify the traffic load carried in each stream.

Figure 46 on page 169 of Chapter 7 "Triple Play and Multiple Streams Testing" illustrates the Streams Pipe display for regular layer 4 traffic streams. When running the TCP Wirespeed application, the display is limited to the six analyzed streams.

You can start and stop traffic from the pipe display. You can also specify the load unit, and use the Configure Streams button to enable specific streams and specify the traffic load carried in each stream.

Understanding the LED panel

When you select a TCP Host or TCP Wirespeed application, the module provides LEDs in the panel for each *analyzed traffic stream*. Figure 44 illustrates the LEDs provided when running the Wirespeed application.

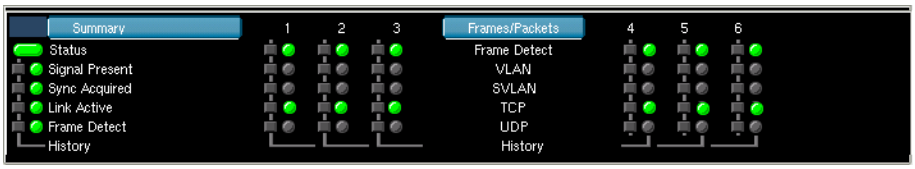


Figure 44 TCP Wirespeed LEDs

Understanding TCP Host and Wirespeed test results

When running the TCP Host and Wirespeed applications, you can observe cumulative test results for the entire link and detailed test results for each analyzed background stream.

Viewing results for a specific stream

You can view detailed test results for a particular stream on the result display by specifying the stream number as the result group, and then selecting the category with the results you want to observe.

Viewing cumulative link results

You can observe cumulative link results for all transmitted streams by selecting the **Link** group, and then the corresponding **Stats**, **Counts**, **Error Stats**, or **AutoNeg Status** category.

Viewing TCP Host results

You can observe summarized and detailed results associated with each TCP connection in the TCP Host result group. IPerf output and layer 3 configuration status results are also available for each connection.

Focusing on key results

Some categories provide so much information you may need to scroll to the right significantly to observe a particular result. To focus on a particular subset of results (and minimize scrolling), you can use the Columns key under the result panes to specify which result columns appear, and hide those you are not interested in. For example, if you want to focus on the delay measurements for each connection, you may choose to hide the Tx Mbps columns or Send Window columns. You can always display them later if you need to.

Configuring the streams

Before running the TCP Host or Wirespeed applications, you must first configure the traffic streams.

To configure the traffic streams

Step1 If you haven't already done so, use the Test Menu to select the Layer 4 Multiple Streams application for the circuit you are testing.

Step2 Configure the streams by doing the following:

a Specify the load unit (see "Enabling multiple streams" on page 172) for traffic carried on the streams.

b Enable the streams you intend to transmit (see "Enabling multiple streams" on page 172), and then specify the traffic load for each stream (see "Specifying the load type for all streams" on page 173).

c Specify the settings that are common to all enabled streams (see "Specifying common traffic characteristics for multiple streams" on page 175).

d Specify the layer 2 (see "Specifying layer 2 stream settings" on page 177), layer 3 (see "Specifying layer 3 stream settings" on page 179), and if applicable, layer 4 settings (see "Specifying layer 4 stream settings" on page 179) for each enabled stream.

You can optionally copy the settings for one stream to all other streams by selecting the **Copy Setups to other Streams** button. Frame or packet characteristics will be copied. Traffic load settings can not be copied; you must specify the type of load (Constant or Ramp) for each individual stream on the Traffic tab.

The actual load for each enable stream is specified on the Load Distribution screen (see "Specifying the load type for all streams" on page 173).

The streams are configured.

Specifying TCP Host settings

Before running the TCP Host or Wirespeed applications, you must specify TCP Host settings. The TCP Host setup tab allows you to configure your instrument as a TCP client or server, and specify key settings such as the TCP port that you are establishing a stateful connection to, the client or server window size, the maximum segment size, and the type of service that the unit is emulating (if your instrument is operating as a client). When configuring the TCP Wirespeed application in Client mode, you can indicate that you want to establish up to 64 connections.

To specify TCP Host settings

Step1 If you haven't already done so, use the Test Menu to select the Layer 4 Multiple Streams or Layer 4 TCP Wirespeed application for the circuit you are testing.

Step2 Select the TCP Host tab, then select the TCP Host Settings sub-tab. Specify the following settings:

Setting	TCP Host Client	TCP Host Server	TCP Wirespeed Client[a]	TCP Wirespeed Server	Value
TCP Host Mode	√	√	√	√	Indicate whether the unit is operating as a **Client**, or as a **Server**.
Connect to Server	√		√		If the instrument is connecting to a server as a client, specify the IP address for the server.
Connect to Port	√		√		The port that the TCP client is connecting to.
Listen Port		√		√	The port that the TCP server is listening on.
Window Size	√	√	√	√	The TCP window size for the connection. Be certain to indicate the unit of measure for the size (KB, MB, or bytes). In Client Mode, the actual window size used may be lower and will be based on the negotiated MSS.
Max Seg Size Bytes	√	√	√	√	The maximum segment size (in bytes) supported by the connection. This is typically 40 bytes less than the maximum transmission unit (to accommodate the TCP/IP header data). The default is 1460 bytes.
Type of Service	√		√		To specify the type of service supported by the connection, select DSCP, then select from the list. The entries show the code points followed by their decimal equivalents in ( ). If you want to transmit traffic without a particular TOS, select TOS. 0x00 will be carried in the TOS field.
Transmit Mode				√	Indicate whether you intend to transmit a specific number of **Bytes**, or traffic for a specific length of **Time**.
Number of Bytes				√	If you set the transmit mode to Bytes, specify the number of bytes you intend to transmit.
Time (sec)				√	If you set the transmit mode to Time, specify the number of seconds that traffic will be transmitted.
Number of Connections			√		Specify the number of connections to the server you want to establish.
Report Rate Format	√	√	√	√	Indicate whether you want the instrument to report throughput in kilobits (Kb), megabits (Mb), kilobytes (KB), or megabytes (MB).
Report Interval	√	√			Specify the interval at which the instrument is to refresh reported test results.

a. Available on the MSAM only. MSAM must be optioned and configured for the Wirespeed application.

The TCP Host settings are specified.

Running the TCP Host application

To run the TCP host

Step1 If you haven't already done so, use the Test Menu to select the Layer 4 Multiple Streams application for the circuit you are testing.

Step2 Specify the settings required to initialize the link (see "Specifying interface settings" on page 46). Be certain to configure a full duplex connection.

Step3 Configure the traffic streams (see "Configuring the streams" on page 160).

Step4 Specify the TCP Host settings (see "Specifying TCP Host settings" on page 160).

Step5 Press **Results** to return to the main screen, and then do the following:

a If you are measuring throughput on an optical circuit, turn the laser on.

b Select the **Actions** tab.

c If your unit is operating as a client, select **Start Traffic**.

d Select **Start TCP Server** or **Start TCP Client** (depending on the mode you specified).

Step6 At a minimum, observe the following test results:

- To verify layer 2 or layer 3 performance, set a result group to **Link**, and then display and observe results in the corresponding **Link Stats** category.
- To verify layer 4 TCP performance, set a result group to **TCP Host**, and then display and observe results in the **L4 Link Stats** and **Output** categories.
- **Throughput**, **Latency (RTD)**, **Packet Jitter**, and **Frame Loss** graphs are also available in the All Streams result group.

TCP throughput is measured. For descriptions of the available result categories, test results, and graphs refer to "CPRI/OBSAI test results" on page 341. You can also optionally create a report detailing the TCP Host settings that you used when measuring TCP throughput.



NOTE:

The tool used to run the TCP Host application may take up to two seconds to launch. This impacts test results derived using the timestamp provided in traffic carrying an ATP payload, such as latency/delay measurements, packet jitter or packet jitter.

Running the TCP Wirespeed application

When configuring the TCP Wirespeed applications, many of the settings are the same as those used to run the TCP Host application. When running TCP Wirespeed, consider the following:

- **Optimal window size**. When turning up TCP service, you can test using a variety of window sizes to determine the size that provides the best layer 4 throughput.
- **Customer traffic emulation**. When running the application, your instrument emulates a true TCP client/server, allowing you to establish up to 64 stateful TCP connections, and collect pertinent throughput, latency, and loss results for many sessions. This provides a more accurate assessment of the network's ability to carry application traffic than layer 3 throughput tests, and provides the data you need to assure customers that issues are not due to poor layer 4 throughput.
- **Filters.** When running the Wirespeed application, filter settings apply to the background streams; they do not impact the TCP connections.

– **Traffic off load**. You can determine whether the proper CoS/QoS settings are specified in the network and verify proper prioritization of background streams by offloading up to four concurrent streams of traffic for analysis.
– **Iperf compatibility.** You can use the TCP Wirespeed application with Iperf to sectionalize TCP performance issues, and demonstrate to the customer that CPE equipment may be the root cause of performance problems.
– **J-Mentor data analysis.** When running the TCP Wirespeed application from 1 Gigabit Optical Ethernet interfaces, you can capture the data, and then analyze it using the J-Mentor application provided on your instrument.

The TCP Wirespeed application is not available for 100 Mbps optical circuits, 802.3 frames, or Q-in-Q encapsulated traffic. IPv6 traffic is also not supported in this release.



NOTE: TCP connections

If you issue a loopup command to an instrument that is actively running the TCP Wirespeed application, the command tears down any TCP connections that were established.

Pressing **Restart** while running the application will not tear down the TCP Connections; it will simply refresh your test results.

To run the TCP Wirespeed application

Step1 Verify that you are not running any other tests.

Step2 If you haven't already done so, use the Test Menu to select the TCP Wirespeed application for the interface you are testing (refer to Table 12 on page 149 for a list of applications).

Step3 Select the **Setup** soft key, and then select the Interface tab to specify the settings required to initialize the link (see "Specifying interface settings" on page 46).

Step4 Configure the traffic streams (see "Configuring the streams" on page 160).

Step5 Specify the TCP Host settings (see "Specifying TCP Host settings" on page 160).

Step6 Press **Results** to return to the main screen, and then do the following:

a If you are measuring throughput on an optical circuit, turn the laser on.

b Select the **Actions** tab.

c If your instrument is operating as a client, select **Start Traffic** to transmit the background streams.

d Select **Start TCP Server** or **Start TCP Client** (depending on the mode you specified).

Step7 At a minimum, observe the following test results:

– To verify layer 2 or layer 3 performance, set a result group to **Link**, and then display and observe results in the corresponding **Link Stats** category.
– To verify layer 4 TCP performance, set a result group to **TCP Host**, and then display and observe results in the **L4 Link Stats** and **Output** categories.
– **Throughput**, **Latency (RTD)**, **Packet Jitter**, and **Frame Loss** graphs are also available in the All Streams result group.

The application is running. When running the TCP Wirespeed application, detailed statistics are provided for each established connection, including bandwidth measurements, delay measurements, window statistics, and frame counts.

TrueSpeed

If your instrument is configured and optioned to do so, you can use it to run the TrueSpeed Test. This test uses the Wirespeed application and automates TCP throughput testing per the IETF draft standard “ippm-tcp-throughput-framework” and to allow TCP throughput testing for up to 64 connections. For more information, see “TrueSpeed Test” on page 321.

7

Triple Play and Multiple Streams Testing

This chapter provides information on testing triple play services and multiple Ethernet (layer 2), IP (layer 3), or TCP/UDP (layer 4) streams of traffic. Topics discussed in this chapter include the following:

– “About Triple Play and Multiple Streams testing” on page 166
– “Multiple Streams testing” on page 167
– “Triple Play testing” on page 181
– “Looping back multiple streams” on page 187
– “Running the TCP Host script” on page 187
– “Playing audio clips” on page 187

About Triple Play and Multiple Streams testing

Before running Triple Play or Multiple Streams applications, be certain you are comfortable configuring and running basic layer 2, layer 3, and layer 4 tests. For details, refer to:

– Chapter 4 “Ethernet and IP Testing” on page 21.
– Chapter 6 “TCP/UDP Testing” on page 147.

Features and capabilities

Features and capabilities include the following when running Triple Play or Multiple Streams applications:

– 10/100/1000 electrical, 1 GigE optical, and 10 GigE LAN testing—You can configure up to ten streams of layer 2, or layer 3, or layer 4 traffic per port, for a total of 20 streams (if your instrument is configured for dual port testing).
– 10 GigE WAN testing—You can configure and transmit up to eight streams of layer 2, layer 3, or layer 4 traffic.
– Uniquely characterize each stream of traffic—For example, you can verify that a network handles VLAN tagged traffic properly by assigning a high priority to one stream, and a lower priority to a second stream.
– IPv6 support—If you purchased the IPv6 Traffic option, you can transmit and analyze multiple streams of IPv6 traffic using the terminate and loopback applications (40G and 100G— Terminate only). When configuring your test, you can specify the required addresses manually, or you can use stateless or stateful auto-configuration to assign addresses for you.
– Triple Play testing—You can transmit and analyze up to seven streams of traffic carrying voice, video, or data payloads to verify triple play service on 10/100/1000, 1 GigE Optical, and 10 GigE LAN circuits.
– When testing triple play, can transmit an actual audio stream (pre-recorded tone or actual voice) to test the audio quality of a triple play network with specific traffic levels before deployment.
– Layer 4 TCP/UDP streams—If you purchased the TCP/UDP option, you can transmit and analyze multiple streams of traffic with TCP or UDP headers in terminate mode. For details, see “Specifying layer 4 stream settings” on page 179.
– TCP throughput measurements—If you purchased the TCP/UDP option, you can establish a TCP connection to a peer, and then measure layer 3 (IP) and layer 4 (TCP) throughput to demonstrate that poor application performance is not due to IP network issues.
– Unique MAC and IP addresses per stream—When running Layer 2 or Layer 3 Triple Play or Multiple Streams applications, you can assign a unique destination MAC and IP address to each individual stream, or you can continue to use the same addresses for all streams. For details, see “Specifying layer 2 stream settings” on page 177 and “Specifying layer 3 stream settings” on page 179.
– Packet capture and analysis—If your instrument is configured and optioned to do so, you can use it to capture transmitted and received data, save it on the instrument or to a USB key, and then either send the data to another technician for analysis, or analyze it yourself using the Wireshark® protocol analyzer (provided on the instrument). For details, see “Capturing packets for analysis” on page 93. In addition, if capturing VoIP packets, the data can by analyzed with the PVA-1000 utility from JDSU.
NOTE: PVA-1000 is used for VoIP analysis only.

– Streamlined filter configuration—Ethernet, IP, and TCP/UDP filter settings are available on the same setup tab, reducing the need to move from tab to tab when you configure your test. For details, see “Filtering received traffic using layer 4 criteria” on page 155.

–When configuring Multiple Streams tests, the Load units can be displayed in either kbps/Mbps or frames per second (fps). Streams pipe displays can also be specified to display in units of fps, kbps or Mbps independently of the Load unit display setting.

Streams Pipe soft key

You can press the **Streams Pipe** soft key to observe summarized test results and information for each individual stream. For details, see “Streams pipe: multiple streams” on page 169 and “Streams pipe: Triple Play streams” on page 182.

Depending on the application you are running, a variety of views are provided for the pipe.

– **Overview**. This view provides key source and destination addresses and the bandwidth received and transmitted for each stream.
– **Addressing**. This view shows the source and destination IP addresses carried in each transmitted stream. The default gateway and subnet mask for each stream are also provided.
– **Traffic Loads**. This view provides more detailed information for the traffic carried in each stream, such as the currently received frame size, the received bandwidth, the transmitted traffic load type (constant or ramped), the transmitted bandwidth, and a count of transmitted Acterna frames.
– **VLAN/VPLS**. These views show key encapsulation data for each stream. For example, if you are analyzing layer 2 Q-in-Q streams, the SVLAN ID and priority for received and transmitted streams appears.

Using the action buttons

The buttons on the Main screen are used to perform actions for *all enabled streams*. For example, if stream 1, stream 2, and stream 3 are enabled, or if you have selected a voice, HDTV, and data stream, pressing the **Start Traffic** button transmits traffic for all three streams simultaneously.

Multiple Streams testing

If your instrument is configured and optioned to do so, you can use it to transmit multiple streams of layer 2, layer 3, or layer 4 traffic. You can configure each individual stream to depict a particular type of traffic, transmit the streams, and then analyze each stream to verify that network routing and switching devices are handling each stream properly (based on the stream’s priority). You can also observe the bandwidth utilized, and a count of transmitted, received, and lost frames for each individual stream.

Multiple Streams test applications

This release supports the Multiple Streams applications listed in Table 13. Loop back applications are listed in Table 13 on page 168 of Chapter 8 “Loop back Testing”.

Table 13 Multiple Streams applications

Circuit	Application	Test Mode
10/100/1000	Layer 2 Multiple Streams	Terminate Dual Terminate[a]
	Layer 3 Multiple Streams	Terminate Dual Terminate[a]
	Layer 4 Multiple Streams	Terminate
100M Optical	Layer 2 Multiple Streams	Terminate Dual Terminate[a]
	Layer 3 Multiple Streams	Terminate Dual Terminate[a]
	Layer 4 Multiple Streams	Terminate
1GigE Optical	Layer 2 Multiple Streams	Terminate Dual Terminate[a]
	Layer 3 Multiple Streams	Terminate Dual Terminate[a]
	Layer 4 Multiple Streams	Terminate
10GigE LAN	Layer 2 Multiple Streams	Terminate
	Layer 3 Multiple Streams	Terminate
	Layer 4 Multiple Streams	Terminate
10GigE WAN	Layer 2 Multiple Streams	Terminate
	Layer 3 Multiple Streams	Terminate
	Layer 4 Multiple Streams	Terminate
100GigE	Layer 2 Multiple Streams	Terminate
	Layer 3 Multiple Streams	Terminate

a. Transport Modules must use two PIMs for the selected interface to test in dual terminate mode. Dual terminate mode is not available when testing 10 Gigabit Ethernet LAN or WAN interfaces using an MSAM.

In addition to the standard Multiple Streams applications, if your instrument is configured and optioned to do so, you can run TCP Wirespeed test applications with up to four streams of layer 4 traffic. For details, see “Running the TCP Wirespeed application” on page 162.

Understanding the LED panel

When you select a Multiple Streams application, the module provides LEDs in the panel for each *enabled traffic streams* (see Figure 45).

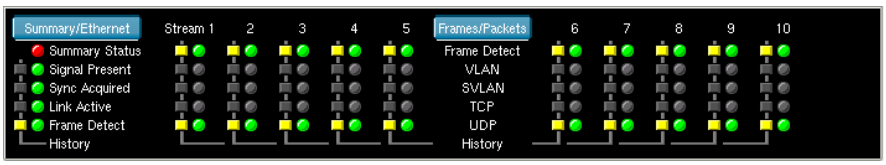


Figure 45 Multiple Stream LEDs (Layer 4)

If you run a Multiple Streams application in Dual Terminate mode, LEDs are provided for both ports.

Streams pipe: multiple streams

When running multiple streams applications, you can use the Streams Pipe soft key to specify the load unit (see "Enabling multiple streams" on page 172), and to access the Load Distribution dialog box. The Load Distribution dialog box is used to enable the streams that you want to transmit (see "Enabling multiple streams" on page 172), and to specify the traffic load carried in each stream (see "Specifying the load type for all streams" on page 173).

Figure 46 illustrates the Streams Pipe display for layer 4 traffic streams.

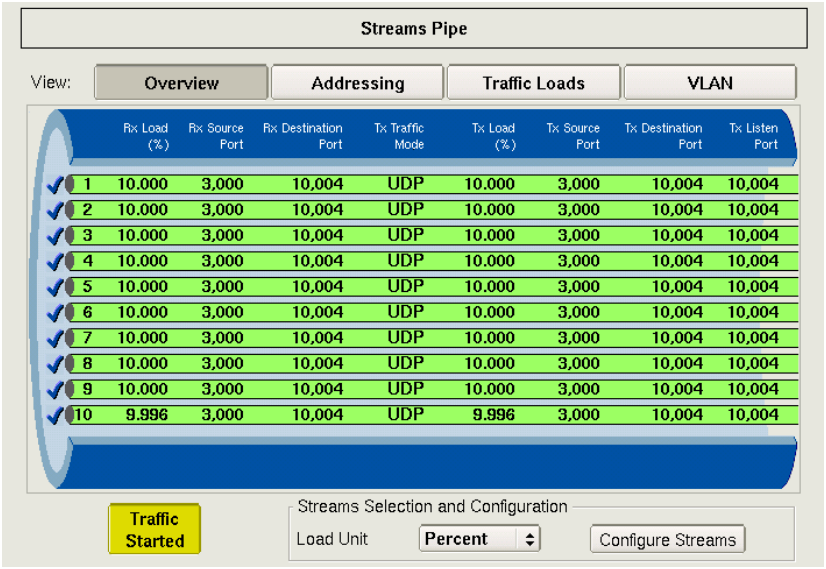


Figure 46 Streams Pipe Display: layer 4 streams

You can start and stop traffic from the pipe display. You can also specify the load and Throughput units, and press the Configure Streams button to enable specific streams, and specify the traffic load carried in each stream.

NOTE:

When observing the pipe for layer 2 or layer 3 traffic, the Frame Length or Packet Size displayed represents the maximum length or size received for each individual stream.

When transmitting multiple VPLS encapsulated streams, the frame length on the Streams Pipe Display represents the customer frame length; the load percentage displayed represents the load as configured for the service provider.

Understanding multiple streams test results

When running Multiple Streams applications, you can observe cumulative test results for the entire link, detailed test results for a particular stream, and graphical results for all analyzed streams.

Viewing results for a specific stream

You can view detailed test results for a particular stream on the result display by specifying the stream number as the result group, and then selecting the category with the results you want to observe. Figure 47 illustrates the L2 Link Results for Stream 1, and the Summary/Status results for all enabled streams.

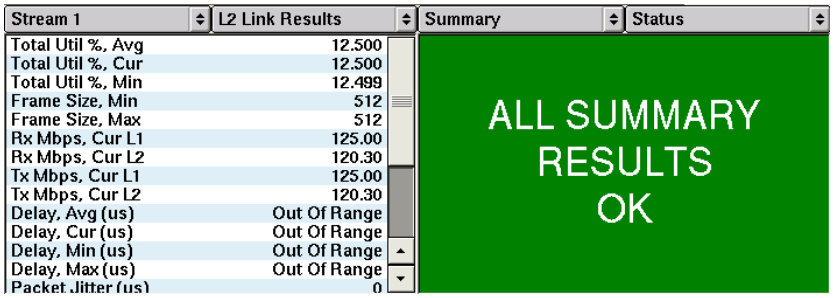


Figure 47 Multiple Streams result display

Viewing cumulative link results

You can observe cumulative link results for all transmitted streams by selecting the **Link** group, and then the corresponding **Stats**, **Counts**, **Error Stats**, or **AutoNeg Status** category.

Viewing graphical results for all streams

Throughput, latency (RTD), packet jitter, and frame loss results can be observed graphically by selecting the **All Streams** group, and then the category with the results you want to observe. When observing graphical results, it's helpful to view the entire result window by selecting **View > Result Windows > Full Size**.

Figure 48 illustrates the Throughput Graph for multiple traffic streams.

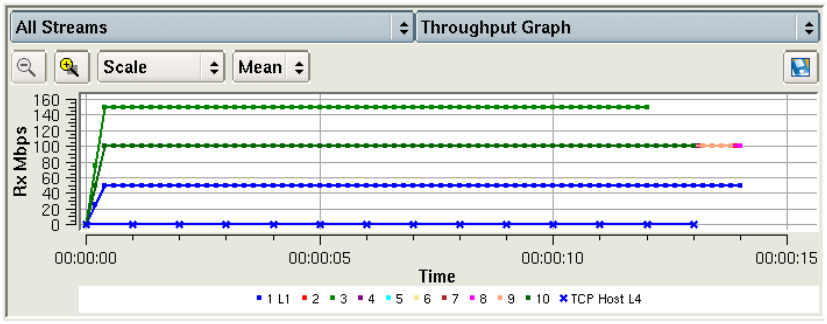


Figure 48 Throughput Graph: Multiple Streams application

A color coded legend appears under the graph indicating which color is used to present results for each of the analyzed streams. In Figure 48, the green lines provide results for Stream 3, the blue lines provide results for Stream 1, and the bright pink line provides results for Stream 8.

Changing graph properties

To simplify the graph, you can select the legend, and then choose the data that you want to observe for each analyzed stream, and hide the rest. You can also focus on a subset of streams by hiding those that you do not want to observe anymore.

To change graph properties

Step1 Select the legend at the bottom of the graph (see Figure 49).



Figure 49 Graph Legend: Multiple Streams application

The Graph properties dialog box appears (see Figure 50 on page 172).

Step2 Under Graph properties, select one of the following:

- Stream
- Frame Size
- CVLAN ID
- SVLAN ID
- MPLS1 ID
- MPLS2 ID



Figure 50 Graph properties dialog box

Step3 Clear the boxes next to the types of streams, the frame sizes, or the SVLAN/CVLAN/MPLS IDs for streams that you do not want to observe.

Step4 Select **Close** to return to the Main screen.

The graph displays data for streams with the selected properties.

Enabling multiple streams

If you selected a Multiple Streams application, you enable streams on the Load Distribution dialog box using the following procedure.

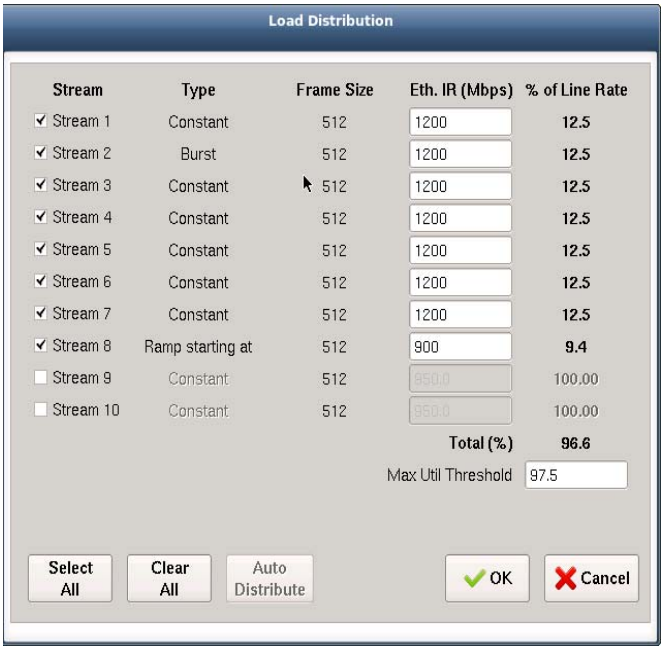
To enable multiple streams

Step1 If you haven't already done so, use the Test Menu to select the Multiple Streams test application for the interface you are testing (refer to Table 15 on page 181 for a list of applications).

Step2 Select the **Streams Pipe** soft key.

Step3 Select **Configure Streams**.

The Load Distribution screen appears.



Step4 Select the streams you want to transmit.

Streams are enabled. If you have already specified the load type for each stream (see “Specifying the load type for all streams” on page 173), you can specify the load.

NOTE:

The **Auto Distribute** button is disabled if one or more traffic streams is configured to transmit a ramped load of traffic.

Specifying the load type for all streams

If you selected a Multiple Streams application, you can transmit a constant load or a ramped load of traffic in any stream.

NOTE:

A single stream may be defined as having a a burst load.See “Specifying the load unit on a stream with burst” on page 174.

To specify the load type for all streams

Step1 If you haven’t already done so, use the Test Menu to select the Multiple Streams test application for the interface you are testing (refer to Table 13 on page 168 for a list of applications).

Step2 Select the **Setup** soft key.

Step3 By default, the module transmits a constant load of traffic for each enabled stream. If this is acceptable, proceed to step 4. If you want to transmit a *ramped* load of traffic for a particular stream or streams, do the following:

a Select the tab corresponding to the stream.

b Select the Traffic sub-tab.

c In Load Type, select **Ramp**, and then specify the time step (in seconds) and the load step (in Mbps, as a percentage of the line rate or in frames per second). For details, see"Transmitting a ramped load" on page 67.

NOTE: When configuring a ramped load of traffic for a stream, the triggers used to stop the ramp *are not available*.

d Repeat step a through step c for each ramped stream of traffic, and then proceed to step 4.

Step4 Select the **Streams Pipe** soft key, and then select **Configure Streams**.

The Load Distribution screen appears.

Step5 Do one of the following:

– If you are transmitting a constant load of traffic for every enabled stream, and you want to distribute the load evenly across the streams, select **Auto Distribute**. The module automatically calculates the load for each stream.

– If you are transmitting one or more ramped streams of traffic, or a combination of constant and ramped loads, enter the load for each enabled stream.

Step6 Select **OK** to store the loads and return to the Streams Pipe dialog box.

Step7 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

The traffic load is specified.

Specifying the load unit on a stream with burst

If a burst signal is necessary in a multiple streams signal, any stream may be defined to carry that bursty signal. Only one stream may be defined as carrying a bursty signal.

Defining a stream as having a Burst load type automatically changes any other stream defined as Burst to the Constant Load Type. It also restricts all enabled streams to be configurable based on Layer 2 bit rate (Eth. IR (Mbps)).

To configure the load unit on a stream with burst load type

Step1 If you haven't already done so, use the Test Menu to select the Multiple Streams test application for the interface you are testing (refer to Table 13 on page 168).

Step2 Select the **Setup** soft KEY.

Step3 Select the **All Streams** tab. Verify that a burst Stream has been specified in the Stream Selection portion of the window. If not specified, select the desired stream from the **Burst Stream** drop-down list**.**

Step4 Select the tab of the individual stream specified as being the Burst Stream.

Step5 On the Traffic tab, select a Load Unit from the drop-down box accessed by clicking the up-down arrows at the end of the Load Unit field.

– If you selected **Burst Time and Information Rate**-

a Enter a desired Burst Time.

b Enter the desired units for the Burst time.

– If you selected **Bytes and Information Rate**-

a Enter the desired Burst Kbytes.Actual Kbytes will be recalculated and will display in the window.

b The Information Rate will display based on the value entered when configuring the individual stream.

– If you selected **Gap Time and Information rate-**

a Enter the Gap Time (period that burst is not being transmitted.)

b The Burst Rate will display based on the value entered.

Specifying the load unit for multiple streams

If you selected a Multiple Streams application, the traffic load for each stream transmitted (except when configured for burst) can be specified in Mbps, or as a percentage of the line rate. If a stream is to be configured with a Burst load type (only one stream may be defined to have a Burst load type), see “Specifying the load unit on a stream with burst” on page 174 for instructions on selecting the load unit on the stream carrying the burst signal.

To specify the load unit

Step1 If you haven’t already done so, use the Test Menu to select the Multiple Streams test application for the interface you are testing (refer to Table 13 on page 168 for a list of applications).

Step2 Select the **Setup** soft key.

Step3 In the Stream Selection section, verify that the Burst Stream is set to None and then under Load Unit, select one of the following:

– **Bit Rate**

– **Percent**

– **Frames Per Second (fps)**

Step4 Select the Allow flooding checkbox to transmit true 100% load in those circuits that can certainly handle the signal.

Step5 If you selected Bit Rate, the Throughput Bit rate definition source must also be specified. Select either **L(ayer)1** (Mbps) or **L(ayer)2** (Eth IR (Mbps)).

The load unit is specified. You can specify the traffic load for each stream (see “Specifying the load type for all streams” on page 173).

Specifying common traffic characteristics for multiple streams

If you selected a Multiple Streams application, common characteristics shared by all streams are specified on the All Streams tab.

To specify traffic characteristics shared by every enabled stream

Step1 If you haven’t already done so, use the Test Menu to select the Multiple Streams test application for the interface you are testing (refer to Table 13 on page 168 for a list of applications).

Step2 Select the **Setup** soft key, and then select the **All Streams** tab.

Step3 Depending upon the application being used, it may be desired to set one of the following:

– **Layer 2 VPLS streams**. If you want to transmit VPLS encapsulated traffic, set VPLS mode to **Enabled**, and then specify the SP source and destination MAC addresses, and the customer's source MAC address.



NOTE:

Although the SP source and destination MAC addresses, and the customer's source MAC address are assigned to every enabled stream, you can specify a unique customer destination MAC address for each individual stream. See "Specifying layer 2 stream settings" on page 177.

– **Layer 2 Non-VPLS streams**. If you do not want to transmit VPLS encapsulated traffic, set VPLS mode to **Disabled**. You can optionally specify source MAC address to be carried in every enabled stream of traffic, or you can specify a unique MAC address for each stream.

  To specify a single address, in Source MAC Mode, select **Single**, and then indicate whether you want to use the factory default address, or specify your own.

  To specify an address for each stream, in Source MAC Mode, select **Per Stream**, and then specify the addresses on the tabs corresponding to each enabled stream (see "Specifying layer 2 stream settings" on page 177).

  To specify the LBM/:LBR traffic mode on Layer 2 Traffic Terminate applications, select **LBM Traffic** from the options in the Test Mode drop-down box. This option is not applicable to VPLS streams and will automatically change VPLS Mode to Disabled, when selected.

– **Layer 3 MPLS streams**. If you want to transmit MPLS encapsulated traffic, set MPLS mode to **Enabled**, and then specify the source MAC address.

  Enable or **disable** ARP mode.

  If you enable ARP mode, specify the source IP for this hop, the destination IP address and subnet mask for the next hop.

  Next, specify source IP address, default gateway, and subnet mask for the customer (Layer 3). These addresses will be used for all enabled streams.

– **Layer 3 Non-MPLS streams**. If you do not want to transmit MPLS encapsulated traffic, set MPLS Mode to **Disabled**, then enable or disable ARP mode.

  In the Layer 3 section of the window, define the Source IP Type. Indicate whether it is desired to use DHCP to assign a single source IP address to all enabled streams, to manually assign a static address to be carried in all enabled streams, or to assign a unique source IP address to each enabled stream.

  To specify a single static address, in Source Type, select **Static**, and then specify the source IP address, default gateway, and subnet mask for the customer.

  To specify an address for each stream, in Source Type, select **Static - Per Stream**, and then specify the addresses on the tabs corresponding to each enabled stream (see "Specifying layer 3 stream settings" on page 179).

– **Layer 4 streams**. Specify the source MAC address, enable or disable ARP mode, and then specify the source IP address, default gateway, and subnet mask for the customer (Layer3). The source MAC and IP addresses will be carried in each enabled stream of traffic.

  Under Layer 4, indicate whether you want to use the unit's source IP address as the ATP Listen IP Address (by setting the ATP Listen IP Type to **Auto Obtained**), or select **User Defined** and then assign your own address. If you do not want to use the default fill pattern (AA) to populate the payloads, specify a different pattern.



NOTE:

The ATP version is set on the "All stream" page. It can be set per stream or all streams. ATPv3 available on the10M/100M/1GbE/10GbE/40G/100G modules.

Step4 To specify the parameters located in the Stream Selection section of the window, follow the procedures for "Specifying the load type for all streams" on page 173, "Specifying the load unit on a stream with burst" on page 174 or "Specifying the load unit for multiple streams" on page 175.

Step5 *40G/100G applications only*. Specify the **Optic Latency Factor.** This setting provides a means to compensate for significant intrinsic delays, especially when using certain types of pluggable optics affecting Frame Delay (latency) measurement results.

In particular, 100G LR4 CFP optics equipped with gearbox functionality have been shown to introduce delays in the range of 70 to 170 nanoseconds. Should this intrinsic delay be deemed significant, the Optic Latency factor allows compensation by specifying a value between 0 and 100 microseconds, with nanosecond granularity. This factor will be subtracted from latency calculations.

To specify the Optic Latency Factor, do the following:

– Run an RTD test with a very short fiber self-loop.

– Enter the returned RTD value in the Optic Latency Factor field on the Setup page.

Step6 *10 GigE applications only*. In **Delay,** indicate whether you want to make measurements using a high degree of precision, or a low degree of precision. In most instances, you should select the high precision setting.

Step7 To specify additional settings for each individual stream, see "Specifying layer 2 stream settings" on page 177, "Specifying layer 3 stream settings" on page 179, or "Specifying layer 4 stream settings" on page 179.

Step8 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

Common traffic characteristics are specified.

Specifying layer 2 stream settings

You can specify the frame type, frame size, and encapsulation settings for each individual stream when configuring standard Multiple Streams applications, or for each type of stream (VoIP, SDTV, HDTV, Data 1, Data 2, Data 3 and Data 4) when configuring Triple Play applications. After specifying settings for a stream (or type of stream), you can optionally copy the settings to every stream.

To specify layer 2 stream settings

Step1 If you haven't already done so, use the Test Menu to select the Multiple Streams, Triple Play, or TCP Wirespeed test application for the interface you are testing (refer to Table 13 on page 168 and Table 15 on page 181 for a list of applications).

Step2 Select the **Setup** soft key, and then select the tab corresponding the stream or type of stream you are configuring.

Step3 Select the **Ethernet** sub-tab, and then specify the frame type, length type, and optional encapsulation settings. For details, refer to:

– "Specifying Ethernet frame settings" on page 49.

– "Configuring VLAN tagged traffic" on page 54.

– "Configuring Q-in-Q traffic" on page 55.

– "Configuring VPLS traffic" on page 55.

Step4 Do one of the following:

– Select the tab corresponding to the next stream or the next type of stream you want to characterize, then repeat step 3.

– *Optional*. If you want to use the same settings for all enabled streams, select **Copy Setups to other Streams**.

Traffic load settings are not copied. Load settings must be configured for each individual stream.

Step5 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

Layer 2 traffic characteristics are specified.

Automatically incrementing configured MAC addresses or VLAN IDs

When configuring layer 2 multiple streams tests, you can indicate that you want the instrument to automatically increment the MAC address and VLAN ID for each stream when you configure the first stream. After you specify the MAC address or VLAN ID for the first stream, you use the **Copy Setups to other Streams** button to copy the values and populate the MAC addresses or VLAN IDs with *incremented* values.

Table 14 shows the values assigned for each stream's MAC address and VLAN ID if the increment options are selected for stream one.

Table 14 Example: Incremented MAC addresses and VLAN IDs

Stream	MAC Address	VLAN ID
1	00-06-5B-15-04-03	2
2	00-06-5B-15-04-04	3
3	00-06-5B-15-04-05	4
4	00-06-5B-15-04-06	5
5	00-06-5B-15-04-07	6

To increment configured MAC addresses or VLAN IDs

Step1 If you haven't already done so, use the Test Menu to select the layer 2 Multiple Streams test application for the interface you are testing (refer to Table 13 on page 168 and Table 15 on page 181 for a list of applications).

Step2 Select the **Setup** soft key, and then enable the streams you intend to transmit (see "Enabling multiple streams" on page 172). Be certain to enable stream 1.

Step3 Select the tab for stream 1, then select the **Ethernet** sub-tab.

Step4 Specify the frame settings (see "Specifying layer 2 stream settings" on page 177), then do the following:

– If you want to increment the configured MAC addresses for the remaining streams, on the graphic of the frame, select **DA**, then specify the destination MAC address for the first stream. Select **Enable Increment During Copy**.

– If you want to increment the configured VLAN ID for the remaining streams, specify VLAN or Q-in-Q as the frame encapsulation, then select **VLAN** on the graphic of the frame. Specify the VLAN ID for the first frame, then select **Enable Increment During Copy.**

Step5 Select **Copy Setups to other Streams**.

The instrument copies the values for stream 1 to each stream, and increments the values for the MAC address or VLAN ID as you specified.

Specifying layer 3 stream settings

When running layer 3 and layer 4 Multiple Streams or layer 3 Triple Play applications, you can specify layer 3 settings for each individual stream or type of stream. After specifying settings for a stream (or type of stream), you can optionally copy the settings to every stream.

To specify layer 3 stream settings

Step1 If you haven't already done so, use the Test Menu to select the Multiple Streams, Triple Play, or TCP Wirespeed test application for the interface you are testing (refer to Table 13 on page 168 and Table 15 on page 181 for a list of applications).

Step2 Select the **Setup** soft key, and then select the tab corresponding the stream or type of stream you are configuring.

Step3 Select the IP sub-tab, and then specify the length type, the packet length, the TOS/DSCP, TTL, and source and destination IP addresses. For details, refer to:

– "Layer 3 testing" on page 78.

– "Configuring MPLS over Ethernet tests" on page 30 (if you are transmitting multiple streams of MPLS encapsulated traffic). MPLS encapsulation is not available when running Triple Play applications.

Step4 Do one of the following:

– Select the tab corresponding to the next stream or the next type of service you want to characterize, then repeat step 3.

– *Optional*. If you want to use the same settings for all streams, select **Copy Setups to other Streams**.

Traffic load settings are not copied. Load settings must be configured for each individual stream.

The source IP address is not copied. If you want to use the same source IP address for each stream, select Static as the Source Type on the All Streams or All Services tab, and then specify the shared Source IP address.

Step5 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

The layer 3 traffic characteristics are specified.

Specifying layer 4 stream settings

When running layer 4 Multiple Streams applications, you can specify layer 4 settings for each individual stream. After specifying settings for a stream, you can optionally copy the settings to every enabled stream.

To specify layer 4 stream settings

Step1 If you haven't already done so, use the Test Menu to select the Multiple Streams or TCP Wirespeed test application for the interface you are testing (refer to Table 13 on page 168 for a list of applications).

Step2 Select the **Setup** soft key, and then select the tab corresponding the stream you are configuring.

Step3 Select the TCP/UDP tab, and then specify the traffic mode (TCP or UDP), the listen port service type (and if applicable, listen port number), the source port number, the destination port number, and the payload (Acterna or Fill Byte). For details, refer to "Specifying layer 4 settings" on page 152.

Step4 Specify the traffic load for the stream (see "Specifying the load type for all streams" on page 173).

Step5 *Optional*. If you want to use the same settings for all enabled streams, select **Copy Setups to other Streams**. *Traffic load settings are not copied*. Load settings must be configured for each individual stream.

Step6 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

The layer 4 traffic characteristics are specified.

Transmitting multiple streams

Before transmitting multiple traffic streams, you must:

– Specify the interface settings required to initialize the link (see "Specifying interface settings" on page 46).
– Specify the load unit for the transmitted traffic (frames per second (fps), Bit Rate or Percent). This setting indicates whether you want to specify the load for each stream in frames per second, as bit rate, or as a percent of the line rate. For details, see "Enabling multiple streams" on page 172.
– Enable the streams you want to transmit (see "Enabling multiple streams" on page 172, or "Specifying layer 2 and layer 3 settings for Triple Play services" on page 186).
– Specify common traffic characteristics for all enabled streams. For example, if you intend to use the factory default source MAC address, and a static IP address as the source addresses for every enabled stream, these are specified on the All Streams tab. For details, see "Specifying common traffic characteristics for multiple streams" on page 175.
– Specify unique traffic characteristics for each enabled stream or type of stream. For example, you can verify that a network handles VLAN tagged traffic properly by assigning a high priority to one stream, and a lower priority to a second stream. Or you can configure and transmit unencapsulated layer 3 VoIP streams and VLAN tagged SDTV streams.

  For details, see "Specifying layer 2 stream settings" on page 177, "Specifying layer 3 stream settings" on page 179, "Specifying layer 4 stream settings" on page 179, and "Specifying layer 2 and layer 3 settings for Triple Play services" on page 186.
– Specify the load for each enabled stream, or let the module automatically distribute the load evenly between enabled streams. For example, if you specify the load unit as a percent and enable 4 traffic streams, selecting **Auto Distribute** distributes a 25% traffic load to each stream. For details, see "Specifying the load type for all streams" on page 173.

If you intend to run the TCP Host application, additional settings are required (see "Running the TCP Host script" on page 187).

If you are running a Triple Play application, see "Transmitting multiple Triple Play streams" on page 186.

To transmit multiple streams

Step1 If you haven't already done so, use the Test Menu to select the Multiple Streams test application for the interface you are testing (refer to Table 13 on page 168 for a list of applications).

Step2 Select the **Setup** soft key, and then select the Interface tab to specify the settings required to initialize the link (see “Specifying interface settings” on page 46).

Step3 Configure the test. For details, refer to:

- “Enabling multiple streams” on page 172.
- “Enabling multiple streams” on page 172.
- “Specifying the load type for all streams” on page 173.
- “Specifying common traffic characteristics for multiple streams” on page 175.
- “Specifying layer 2 stream settings” on page 177.
- “Specifying layer 3 stream settings” on page 179.
- “Specifying layer 4 stream settings” on page 179.

Step4 Select **Results** to return to the Main screen.

Step5 Select **Start Traffic** to transmit the streams over the circuit.

Multiple streams are transmitted. For an overview of the test results presented when transmitting multiple streams, see “Understanding multiple streams test results” on page 170.

SAMComplete

If your instrument is configured and optioned to do so, you can use it to run the SAMComplete test. This test is a multi-stream test based on ITU-T Y.156sam that performs a two-phase test. First, the test verifies whether each Ethernet service is properly configured. Second, multiple Ethernet service instances are verified simultaneously, each meeting its assigned Committed Information Rate (CIR). See “SAMComplete” on page 304.

Triple Play testing

If your instrument is configured and optioned to do so, you can use it to transmit and analyze traffic emulating Triple Play services. When running Triple Play applications, you can configure each type of stream (voice, video, or data) with unique layer 2 or layer 3 characteristics. For example, if you are running a Layer 3 Triple Play application, you can setup all voice streams to use Q-in-Q encapsulation, all SDTV (or HDTV) video streams to use VLAN tags, and all data streams to use no encapsulation. You can also transmit an actual audio stream (pre-recorded voice, tone, or voice conversation) to test the audio quality of a triple play network with specific traffic levels before deployment.

Triple Play test applications

This release supports the Triple Play applications listed in Table 15.

Table 15 Triple Play applications

Circuit	Application	Test Mode
10/100/1000	Layer 2 Triple Play	Terminate
	Layer 3 Triple Play	Terminate
100M Optical	Layer 2 Triple Play	Terminate
	Layer 3 Triple Play	Terminate

Table 15 Triple Play applications (Continued)

Circuit	Application	Test Mode
1GigE Optical	Layer 2 Triple Play	Terminate
	Layer 3 Triple Play	Terminate
10GigE LAN	Layer 2 Triple Play	Terminate
	Layer 3 Triple Play	Terminate

Understanding the LED panel

When you select a Triple Play application, the module provides LEDs in the panel for *each type of traffic* transmitted in *each enabled stream* (see Figure 51).

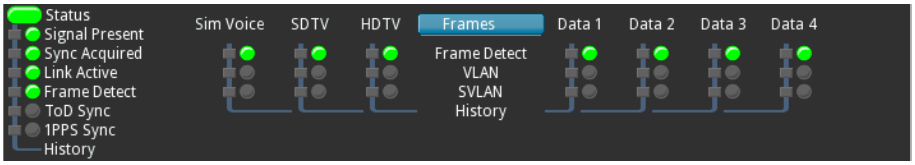


Figure 51 Triple Play LEDs (Layer 3)

Streams pipe: Triple Play streams

Figure 52 illustrates the Streams Pipe Display for Layer 3 Triple Play streams.



Figure 52 Streams Pipe Display: Layer 3 Triple Play streams

You can start and stop traffic directly from the pipe display. You can set the Throughput units display to kpbs or Mbps. You can also press the **Configure Triple Play Services** button to select the type of services you want to emulate, and specify parameters for each type. For example, if you are emulating voice service, you can specify the Codec, sampling rate, and the number of calls.

Understanding Triple Play test results

When running Triple Play applications, you can observe cumulative test results for the entire interface and link. You can also observe throughput, latency (RTD), packet jitter, and frame loss graphs for all analyzed streams.

Viewing cumulative link results

You can observe cumulative link results for all transmitted streams by selecting the **Link** group, and then the corresponding **Stats** or **Counts** category.

Viewing graphs

Throughput, latency (RTD), packet jitter, and frame loss results can be observed graphically by selecting the **Graphs** group, and then the category or the results that you want to observe. When observing the graphs, it's helpful to view the entire result window by selecting **View > Result Windows > Full Size**.

Figure 53 illustrates the Throughput Graph for Triple Play streams.

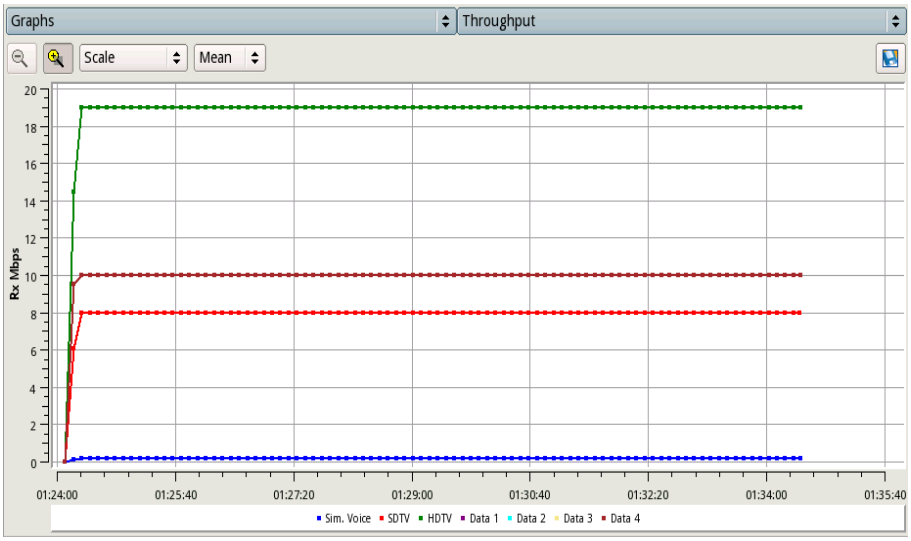


Figure 53 Throughput Graph

A color coded legend appears under the graph indicating which color is used to present results for each type of analyzed streams. In Figure 53, the green line provides results for HDTV traffic, the red line provides results for SDTV traffic, and the purple and light blue lines provide results for the data traffic. The bright blue line provides results for simulated voice traffic. **NOTE:** The bright blue reflects simulated voice, not the audio frames.

Changing graph properties

If you would like to focus on results for a specific type of stream, frame size, CVLAN, SVLAN, or VLAN ID, you can change the graph properties.

To change graph properties

Step1 Select the legend at the bottom of the graph (see Figure 54).

Figure 54 Graph Legend: Triple Play application

The Graph properties dialog box appears.

Step2 Under Graph properties, select one of the following:

- Stream
- Frame Size
- CVLAN ID
- SVLAN ID
- VLAN ID

Step3 Clear the boxes next to the types of streams, the frame sizes, or the SVLAN/CVLAN/VLAN ID for streams that you do not want to observe.

Step4 Select **Close** to return to the Main screen.

The graph displays data for streams with the selected properties.

Characterizing Triple Play services

Before transmitting multiple streams of Triple Play traffic, you must characterize each type of service, and indicate the number of calls (VoIP), channels (SDTV and/or HDTV), and data streams that you intend to transmit and analyze.

The maximum utilization threshold is equal to the line rate for the application; therefore, if you utilize all of the bandwidth for one type of stream, you can not transmit the other types concurrently.

To characterize each type of service

Step1 If you haven't already done so, use the Test Menu to select the Triple Play test application for the interface you are testing (refer to Table 15 on page 181 for a list of applications).

Step2 Select the **Setup** soft key, and then select the **All Services** tab.

Step3 Do one of the following:

- **Layer 2 Triple Play**. To specify a single source MAC address shared by all streams, in Source MAC Mode, select **Single**, and then indicate whether you want to use the factory default address, or specify your own.

  To specify a source MAC address for each stream, in Source MAC Mode, select **Per Stream**, and then specify the addresses on the tabs corresponding to each type of service (see "Specifying layer 2 and layer 3 settings for Triple Play services" on page 186).

- **Layer 3 Triple Play**. Under MAC Address setup, indicate whether you want to use the factory default address, or specify your own.

  Under Customer Information, in Source Type, indicate whether you want to use DHCP to assign a single source IP address to all streams (for all services), manually assign a static address to be carried in streams for all services, or assign a unique source IP address to each stream.

  To specify a single static address, in Source Type, select **Static**, and then specify the source IP address, default gateway, and subnet mask for the customer.

To specify an address for each stream, in Source Type, select **Static - Per Stream**, and then specify the addresses on the tabs corresponding to each type of service (see "Specifying layer 2 and layer 3 settings for Triple Play services" on page 186).

Step4 Press **Configure Triple Play Services**. The Define Triple Play Services dialog box appears. Specify the following:

– **Voice service**. If you intend to simulate and analyze voice traffic, select the checkbox next to **Simulated**. If your instrument includes the VoIP option, a second voice selection is available. Choose **Voice Conversation**, **IP Voice Announce**, or **Transmit Tone**. Specify the Codec, sampling rate (in ms), and the number of calls to emulate. Your instrument automatically calculates the bandwidth utilized by each call (in kbps), the total rate (in Mbps) for all calls, and the frame size (in Bytes).

NOTE: Increasing the sampling rate reduces required bandwidth; increasing the number of calls utilizes additional bandwidth. If you utilize all of the bandwidth for voice data, you can not transmit SDTV, HDTV, or data traffic at the same time.

IMPORTANT: The Codec type on the receiving and transmitting unit must match for the audio to work properly.

– **Video service**. If you intend to emulate and analyze SDTV and/or HDTV traffic, select the corresponding checkbox, and then specify the number of channels, and the compression rate (MPEG-2, at 4.00 Mbps or 19.00 Mbps, or MPEG-4, at 2.00 Mbps or 7.00 Mbps).

NOTE: Each additional SDTV channel increases the rate by 4.0 or 2.0 Mbps. Each additional HDTV channel increases the rate by 19.0 or 7.0 Mbps. If you utilize all of the bandwidth for video data, you can not transmit voice and data traffic with the video traffic.

– **Data streams**. If you intend to emulate and analyze data traffic, select any, or all of the four checkboxes, and then configure the rate (up to the maximum utilization threshold), and a constant or ramped load of traffic for the selected data streams. If you select Ramp, specify the Time Step (in seconds) and Load Step (in fps or Mbps). Finally, specify the frame size to transmit (in Bytes), or select the Random check box to transmit frames of randomly generated sizes.

– After specifying the settings, select the OK button to return to the setup menu.

Step5 Select the **Voice** tab, and then in the left pane, select **Audio Codec**.

Step6 Specify the following settings:

Setting	Description
Primary Codec	Select the codec type to be advertised/supported for receiving audio packets. **IMPORTANT:** The Codec type on the receiving and transmitting unit must match for the audio to work properly.
Speech Per Frame	Specify the number of milliseconds of speech per transmission frame the unit will transmit.
Jitter buffer	Set the jitter buffer length.This is the number of milliseconds of speech that will be collected before an attempt will be made to play the speech back. This allows lost, late, or out-of-sequence packets time to arrive and be reassembled before playback.
Transmit Source	Select the transmit source: Voice conversation (transmits and receives live voice), IP voice announce (the unit repeats a sequence of words including the calling party's IP address), Tone (transmits the specified frequency).
Language	If the Transmit Source is set to IP Voice Announce, the Language selection becomes available. This specifies the language for the transmitted voice announcement.

Setting	Description
Silence Suppression	Specify whether silence suppression is enabled.

Step7 In the left panel on the side of the tab, select **QoS** and then specify the following:

Setting	Description
MOS Scaling	Specify the scale used for MOS results.
Jitter Threshold	Specify the pass and fail thresholds for the jitter result.
Delay Threshold	Specify the pass and fail thresholds for the delay result.
Loss Threshold	Specify the pass and fail thresholds for the loss result.
Content Threshold	Specify the pass and fail thresholds for the MOS results.

Step8 If you do not need to specify other settings, select the **Results** soft key to return to the Main screen.

Triple Play service is characterized.

Specifying layer 2 and layer 3 settings for Triple Play services

You can specify layer 2 and layer 3 settings for each type of service on the Voice, SDTV, HDTV, Data 1, Data 2, Data 3,and Data 4 setup tabs. For details, see:

– “Specifying layer 2 stream settings” on page 177
– “Specifying layer 3 stream settings” on page 179

Transmitting multiple Triple Play streams

Before transmitting multiple Triple Play streams, you must:

– Specify the interface settings required to initialize the link (see “Specifying interface settings” on page 46).
– Specify setting that characterize each type of service, and indicate the bandwidth utilized by each type (see “Characterizing Triple Play services” on page 184).
– Specify layer 2 and layer 3 settings for the streams (see “Specifying layer 2 stream settings” on page 177 and “Specifying layer 3 stream settings” on page 179).

To transmit multiple Triple Play streams

Step1 If you haven’t already done so, use the Test Menu to select the Triple Play test application for the interface you are testing (refer to Table on page 181 for a list of applications).

Step2 Select the **Setup** soft key, and then select the Interface tab to specify the settings required to initialize the link (see “Specifying interface settings” on page 46).

Step3 Configure the test. For details, refer to:

– “Characterizing Triple Play services” on page 184.
– “Specifying layer 2 and layer 3 settings for Triple Play services” on page 186.

Step4 Select **Results** to return to the Main screen.

Step5 Select **Start Traffic** to transmit the streams over the circuit.

Multiple Triple Play streams are transmitted. For an overview of the test results presented when transmitting Triple Play traffic, see “Understanding Triple Play test results” on page 183.

Looping back multiple streams

Loop back testing allows you to transmit traffic from one JDSU Ethernet test set, and then loop the traffic back through a second unit on the far end of a circuit. For details, refer to Chapter 8 “Loop back Testing”.

Running the TCP Host script

When running layer 3 and layer 4 multiple streams applications, you can configure and run the TCP Host script to establish a stateful TCP connection with another device, and then determine the TCP throughput, window size and latency associated with the connection.

For details, refer to “Running TCP Host or Wirespeed applications” on page 158.

Playing audio clips

When running layer 3 triple play applications, you can transmit an actual audio stream (pre-recorded voice, tone, or voice conversation). This allows testing of the audio quality of a triple play network with specific traffic levels before deployment.

To play audio clips

Step1 If you haven’t already done so, use the Test Menu to select the layer 3 Triple Play test application for the interface you are testing (refer to Table on page 181 for a list of applications).

Step2 Select the **Setup** soft key, and then select the All Services tab.

Step3 Tap the **Configure Triple Play Services** button.

The Define Triple Play Services dialog box appears

Step4 In the Voice section, do the following:

a Select one or both Voice types:

– **Simulated**—a stream of Acterna test packets.

– Choose one of the following:
- **Voice Conversation**—typical voice call
- **Transmit Tone**—a single frequency tone transmitted via RTP packets
- **IP Voice Announce**—pre-recorded audio clip transmitted via RTP packets

b Specify the Codec, sampling rate (in ms), and the number of calls to emulate, as described in step 4 on page 185.

IMPORTANT: The audio will work properly only when the Codec type matches on the receiving and transmitting unit.

Step5 Verify the settings on the Voice tab, as described in step 5 on page 185.

Step6 Select the **Results** soft key to return to the test result menu.

Step7 Select the **Play Audio** action button to transmit the audio stream.

Step8 Verify the audio by doing the following:

- Observe the **Audio Detect** LED. It illuminates when audio packets are received.
- Observe the **Sim. Voice** LED.
- Use a headset to listen to the audio.



NOTE:

If playing audio on a MTS8000 with DMC, no audio path is available. You can use the simulated voice and observe results but will not hear audio.

8

Loop back Testing

This chapter provides information on looping back Ethernet, IP, TCP/UDP, Fibre Channel, and multiple streams of traffic.

Topics discussed in this chapter include the following:

– “About Loop back testing” on page 190
– “Specifying a unit identifier” on page 195
– “Using LLB to loop received traffic back to the local unit” on page 195
– “Using Loop Up to initiate a loop back from the local unit” on page 197

About Loop back testing

If your instruments are configured and optioned to do so, you can use two Transport Modules (or other JDSU compliant Ethernet test instruments) to transmit Ethernet, IP, TCP/UDP, or Fibre Channel traffic from one instrument, and then loop the traffic through a second instrument back to the sending instrument. By transmitting and then looping traffic back, you are essentially emulating a longer circuit on the network.

Before looping back traffic, it is important to understand the terminology and concepts in the following sections.

Loop back terminology

The following terms are used to explain loop back testing in this chapter.

Local unit

Used in this chapter to refer to the traffic-originating unit (which is always placed in Terminate mode).

Loop back unit

Used in this chapter to refer to the unit that loops received traffic back to the traffic-originating (local) unit. If the loop back unit is capable of generating traffic, place it in terminate mode when you want to loop traffic through to the transmitter. If the loop back unit is not capable of generating traffic (it is a loop back-only unit), place it into loop back mode.

Terminate mode

Mode used for loop back applications when both the local unit and the loop back unit are capable of *generating traffic*. Also used by local unit to generate traffic that will be looped back by a unit that is only capable of looping received traffic back. In this scenario, the loop back unit is placed in loop back mode.

All Dual Module Carrier, Transport Module, and MSAMs and Transport Modules with Ethernet testing capability are shipped with the ability to generate and transmit traffic; therefore, when running loop back applications using two Dual Module Carrier, Transport Module, and MSAMs, two Transport Modules, or an MSAM and a Transport Module, both instruments should be placed in terminate mode.

Loop back mode

Previously, loop back tests were always performed with both the local traffic transmitting unit and the loop back unit in *Terminate* mode. Assuming both units can transmit traffic, this is still the case.

When you purchase an Multiple Services Application Module, you can order a unit that is capable of generating, transmitting, and analyzing Ethernet traffic, or you can order a unit that simply loops back traffic received from another transmitting unit. The loop back unit is not capable of generating its own traffic; it functions simply as a *loop back device*.

If you are using a loop back-only unit at the far end, you must place the local unit in *Terminate* mode; the loop back unit must be placed in *Loop back* mode. Configure and transmit traffic from the local unit just as you would for an end-to-end test; and verify that the *filter settings on the loop back unit* will allow traffic to pass from its receiver through to its transmitter.

You can still initiate the loop back from your local unit using the **Loop Up** action button, or you can actively loop traffic back from the loop back unit using the **LLB** action button.

Key loop back concepts

The following concepts apply when configuring loop back applications.

ARP settings

If you are looping back layer 3 or layer 4 traffic, and you want to use ARP to obtain the units MAC addresses, be certain to enable ARP on *both units*.

If ARP is *disabled* on all units on the circuit, you can issue a broadcast request to *loop up the first device that responds* (rather than a specific unit).

Address swapping

On the loop back unit, received frames and packets are looped through to the transmitter after the destination and source MAC addresses (layer 2, 3, and 4 loop backs), IP addresses (layer 3 and 4 loop backs), and if applicable, port numbers (layer 4 loop backs) are swapped.



NOTE:

Applications using the100G interface do not automatically swap addresses for traffic transmitted from the loop back unit.

Filter criteria on the loop back unit

Only Unicast frames that pass the filter criteria specified on the loop back unit are looped back to the local unit.

If the Ethernet filter settings are all Don’t Care, and/or the IP and TCP/UDP filters are both disabled, traffic carrying *any payload* will pass through the filter for analysis.

Loop types

When configuring the local traffic-generating unit, you can specify that you want to issue a Unicast loop-up command, or a Broadcast loop-up command.

If you are running an Ethernet application, Unicast commands are used to loop up a specific test instrument on the far end; Broadcast commands are used to loop up the first instrument on the circuit that responds.

If you are running a Fibre Channel application, and you suspect that a switch on the circuit you are testing discards Broadcast frames, be certain to specify a Unicast loop type. Otherwise, the switch will discard the Broadcast loop up frame, and the unit on the far end will not be looped up.

LBM Traffic

Used for Loop back Message/Loop back Reply (LBM/LBR) frame analysis where the far-end unit (any equipment that responds to LBM messages) loops back any packet containing the LBM message.

VLAN and Q-in-Q traffic

The loop back unit uses the same IDs and priorities assigned to the received traffic, and loops the traffic back on the same virtual LAN using the same priority.

VPLS labels

The labels for traffic received by the loop back unit are replaced with *the labels specified for transmitted traffic on the Ethernet tab* before the traffic is passed through to the loop back unit's transmitter.

If you are looping back multiple streams of VPLS traffic, you can specify a unique tunnel label and VC label for each individual stream, or you can specify the labels for one stream, and then copy them to the other streams.

VPLS service provider and customer destination addresses

When looping back VPLS traffic, the loop back unit swaps the service provider destination address (SP DA) and service provider source address (SP SA) carried in received traffic before looping the traffic through to the transmitter. When configuring traffic on the local unit, you must specify the service provider source address of the loop back unit as the service provider destination address for all traffic transmitted from the local unit. This is because when looping back VPLS traffic, the local unit will not issue a broadcast request to loopup the next JDSU Ethernet test instrument on the circuit. Essentially, you must tell it to loop up a specific test instrument by specifying the correct service provider DA.

Where are the VPLS addresses specified?

The SP destination address is specified on the Ethernet tab by selecting the **DA** field for the service provider frame; the customer destination address is specified by selecting the **Data** field for the SP frame, and then selecting the DA field for the customer frame (displayed graphically underneath the SP frame).

Looping back multiple streams of VPLS traffic.

If you are looping back multiple streams of VPLS traffic, you must specify a destination SP address for *all enabled streams* (on the All Streams tab), but you can specify a unique customer destination address f*or each individual stream* on it's corresponding setup tab. You can also copy the customer destination address for one stream to all enabled streams.

MPLS labels

Before received traffic is passed through to the loop back unit's transmitter, the labels for the traffic are automatically replaced with *the labels specified for traffic transmitted from the loop back unit*; therefore:

– If your local unit is configured to transmit traffic with a second MPLS label, but the loop back unit is configured to transmit traffic with a single label, the out of sequence and lost frames counts reported by the local unit may increment if the incoming frame rate is too high.

– If your local unit is configured to transmit traffic with a single MPLS label, but the loop back unit is configured to transmit traffic with a second label, the local unit's receive bandwidth utilization will exceed its transmitted bandwidth utilization.



NOTE:

Applications using the100G interface do not automatically replace labels specified for traffic transmitted from the loop back unit.

If you are looping back multiple streams of MPLS traffic, you can specify unique labels for each individual stream, or you can specify the labels for one stream, and then copy them to the other streams.

MPLS destination addresses

If you initiate a loop back from a local unit using the **Loop Up** button, and ARP is enabled on both units, you must specify the destination IP address and subnet mask for the next hop on the circuit.

If you use the **LLB** button on the loop back unit to loop traffic back to the local unit, and ARP is enabled on both units, you must manually specify the destination IP addresses for the traffic transmitted from the local unit and for the traffic looped back by the loop back unit.

If ARP is disabled, you must also specify the destination MAC address for traffic transmitted by the local unit.

If you are looping back multiple streams of MPLS traffic, and ARP is disabled, you can specify a unique destination MAC address (on the Ethernet tab), and a unique destination IP address (on the IP tab) for each individual stream, or you can specify the addresses for one stream, and then copy them to the other streams.

TCP/UDP ATP Listen IP Address and Listen Port

The Transport Module and Multiple Services Application Module use an *ATP Listen IP Address* and *ATP Listen Port* to determine whether received layer 4 traffic carries an ATP payload.

If you issue a **Loop Up** command from a local unit, after the local unit receives a response from the loop back unit indicating that the loopup was successful, the local unit's ATP Listen IP Address and ATP Listen Port are automatically set to the destination IP address and destination port number carried in the looped back traffic. The loop back unit's ATP Listen IP Address and ATP Listen Port will also automatically be set to the destination IP address and destination port carried in the traffic it receives from the local unit.

If you use the **LLB** action button on the loop back unit, it is essential that you specify the destination IP address and port carried in received traffic as the ATP Listen IP Address and ATP Listen Port when you configure tests that require an ATP payload (such as delay measurements, out of sequence counts, lost frames counts, and packet jitter measurements).

Understanding the graphical user interface

When running loop back tests, the user interface looks much like it does for standard end-to-end or multiple streams tests.

Loop back action buttons

Three action buttons are used for the purpose of initiating or ending loop back tests, and placing a unit into loop back mode.

Loop Up

Press **Loop Up** when you want to initiate the loopup of another unit on the circuit from your unit. In this scenario, you are initiating the loopup from the *local unit*.

Loop Down

Press **Loop Down** when you want to end the loopup of another unit on the circuit. In this scenario, you are ending the loopup from the *local unit*.

LLB

Press **LLB** to loop received traffic back through to a units transmitter, or to stop looping traffic back through to the transmitter. In this scenario, you are initiating or ending the loopup from the *loop back unit* itself.

Loop back messages

During loop back testing, if you initiate or end the loop back from the local unit using the **Loop Up** and **Loop Down** actions, messages are sent to each loop back partner indicating the status of the loop back. These messages appear in the Message Bar provided on the Main screen of the user interface.

When you configure your unit for a loop back test, you can specify a “Unit Identifier” which will be provided in each loop up or loop down frame sent from the unit.

Loop back tests

If your instrument is configured and optioned to do so, you can run a loop back test using each of the applications listed in Table 16.

Table 16 Applications used for loop back testing

Application[a]	10/100/1000	100 FX Optical Ethernet	1 GigE Optical Ethernet or Fibre Channel	2 Gig, 4 Gig or 8 Gig[b] Fibre Channel	10 GigE LAN Ethernet	10 GigE WAN Ethernet
Layer 2 Traffic	√	√	√	√	√	√
Layer 2 Multiple Streams	√	√	√	N/A	√	√
Layer 3 Traffic	√	√	√	N/A	√	√
Layer 3 Multiple Streams	√	√	√	N/A	√	√
Layer 4 Traffic	√	√	√	N/A	√	N/A
Layer 4 Multiple Streams	√	√	√	N/A	√	N/A

a. If both units are capable of generating traffic, select a Terminate mode application for each unit. If the loop back unit cannot generate traffic, place it in Loop back mode.
b. 8Gigabit Fibre Channel XFPs require an MSAMv2 for proper operation.

You can also loop back layer 2 and layer 3 traffic when running NextGen applications carrying a GFP payload.

Specifying a unit identifier

You can specify an identifier to be carried in all loop up and loop down frames originating from your unit. This allows a technician on the far end to determine where the loop commands came from.

The default identifier for the Dual Module Carrier, Transport Module, and MSAM is “JDSU 6000”. The default identifier for the Transport Module is “JDSU 8000”.

To specify a unit identifier

Step1 If you haven’t already done so, use the Test Menu to select the application for the interface you are testing.

Step2 Select the **Setup** soft key, and then select the Interface tab.

Step3 Select the Unit Identifier setting, and then type the identifier using up to 25 characters.

The identifier is specified.



NOTE:

If you are observing loop up or loop down messages on another Transport Module or MSAM, the full unit identifier appears in the messages. If you are observing the messages on other JDSU Ethernet testers, such as the FST-2802 or the HST (with an Ethernet SIM), the identifier will be truncated, and will display only the first ten characters.

Using LLB to loop received traffic back to the local unit

You can loop received traffic through to a unit’s transmitter and back to the local (traffic-originating) unit by selecting the LLB action button provided on the loop back unit.

To loop received traffic back using LLB

Step1 If you haven’t already done so, on both units, launch the layer 2, layer 3, layer 4, triple play, or multiple streams application for the circuit you are testing (see “Step 1: Selecting a test application” on page 2).

If you are looping back traffic on an Ethernet circuit, and both units are capable of transmitting traffic, place each in **Terminate** mode; otherwise, if the loop back unit is not capable of generating traffic, place it in **Loop back** mode.

If you are looping back traffic on a Fibre Channel circuit, place both units into **Terminate** mode. Loop back mode is not available for Fibre Channel applications.

Refer to the sections below for a list of available applications:

- “Ethernet and IP test applications” on page 26
- “MiM applications” on page 27
- “TCP and UDP applications” on page 149
- “Multiple Streams testing” on page 167
- “Fibre Channel test applications” on page 250

Step2 On the local unit, specify the link initialization settings.

– If you are looping back traffic on an Ethernet circuit, see "Specifying interface settings" on page 46.

– If you are looping back traffic on a Fibre Channel circuit, see "Specifying interface settings" on page 252.

Step3 On the local unit, specify the settings for transmitted traffic.

If you are looping back a single stream of layer 2 traffic, refer to one of the following:

– "Layer 2 testing" on page 46

– "Configuring layer 2 MAC-in-MAC tests" on page 126

– "Configuring layer 2 Fibre Channel tests" on page 252

If you are looping back a single stream of layer 3 traffic, refer to the following:

– "Layer 2 testing" on page 46

– "Layer 3 testing" on page 78

If you are looping back a single stream of layer 4 traffic, refer to the following:

– "Layer 2 testing" on page 46

– "Layer 3 testing" on page 78

– "Specifying layer 4 settings" on page 152

If you are looping back multiple streams of traffic, refer to the following as appropriate for your application:

– "Enabling multiple streams" on page 172

– "Specifying layer 2 stream settings" on page 177

– "Specifying layer 3 stream settings" on page 179

– "Specifying layer 4 stream settings" on page 179

– "Specifying layer 2 and layer 3 settings for Triple Play services" on page 186

Step4 On the loop back unit, do the following:

a If you are running a single-stream application, verify that the applicable filter settings are either disabled, set to **Don't Care**, or that they match the settings for the traffic transmitted from the local unit.

b On the Main screen, select the Actions tab, and then select **LLB**.

Step5 On the local unit, select the Actions tab, and then select one of the following:

– **Start Traffic** (if you configured a constant or bursty load).

– **Start Ramp** (if you configured a ramped traffic load).

When the loop back unit receives the traffic, it does the following:

– Determines which frames or packets satisfy its filter criteria. Only traffic that satisfies the criteria will be looped back to the near end unit.

– Swaps the destination and source addresses or port IDs, and if applicable, port number for every frame or packet it receives.

– Transmits the traffic back to the local unit.

Traffic is looped back to the local unit.

Using Loop Up to initiate a loop back from the local unit

You can select the Loop Up button on the local (traffic generating) unit to loop up another unit on the circuit. After sending the Loop Up frame, a confirmation message from the loop back unit appears in the message bar of the Main screen of your local unit informing you that the loop back is successful.

Before sending the Loop Up frame, your unit must be configured as follows:

– If you are looping back layer 2 non-VPLS Ethernet traffic, the near end unit automatically detects the MAC address for the next unit on the circuit; therefore, you do not need to configure the destination MAC address. It will be populated automatically for you.

  If you want to loop up a specific device, you can specify that you are using a Unicast loop type, and then specify the destination MAC address for the device you are looping up.

– If you are looping back layer 2 Fibre Channel traffic, the near end unit automatically detects the source port ID for the next Fibre Channel port on the circuit; therefore, you do not need to configure the destination port ID (D_ID). It will be populated automatically for you.

– If you are looping back layer 3 traffic, you must specify the source IP address for the unit on the far end of the circuit as the destination IP address for traffic transmitted by the local unit.

  Be certain to specify the same destination address for the filter on the receiving loop back unit.

– If you are looping back layer 3 or layer 4 traffic, and you want to use ARP to populate the units MAC addresses; be certain to enable ARP on *both units*.

– If you are looping back layer 4 traffic, after you issue the Loop Up command (from the local unit), and the unit receives a response from the far end unit indicating that the loopup was successful, the local unit's ATP Listen IP Address and ATP Listen Port are automatically set to the destination IP address and destination port number carried in the looped back traffic. The far end unit's ATP Listen IP Address and ATP Listen Port will also automatically be set to the destination IP address and destination port carried in the traffic it receives from the local unit.

– You can optionally specify unit identifiers for each unit (for example, "SamsUnit" and "JoesUnit"). When the units send confirmation messages to each other indicating the status of the loop back, the messages will identify each unit using the identifier. For details, see "Specifying a unit identifier" on page 195.

To initiate a loop back from the local unit

Step1 If you haven't already done so, launch the layer 2, layer 3, layer 4, triple play, or multiple streams application for the circuit you are testing (see "Step 1: Selecting a test application" on page 2). Refer to the sections below for a list of available applications:

  – "Ethernet and IP applications" on page 26
  – "MiM applications" on page 27
  – "TCP and UDP applications" on page 149
  – "Multiple Streams testing" on page 167

Step2 On the local unit, specify the link initialization settings (see "Specifying interface settings" on page 46).

Step3 On the local unit, specify the settings for transmitted traffic. Depending on the application you selected, see:

- "Layer 2 testing" on page 46
- "Layer 3 testing" on page 78
- "Configuring layer 2 MAC-in-MAC tests" on page 126
- "Specifying layer 4 settings" on page 152
- "Enabling multiple streams" on page 172
- "Specifying layer 2 stream settings" on page 177
- "Specifying layer 3 stream settings" on page 179
- "Specifying layer 4 stream settings" on page 179
- "Specifying layer 2 and layer 3 settings for Triple Play services" on page 186

Step4 If you are looping back a single stream of non-VPLS layer 2 traffic, proceed to step 8.

Step5 If you are looping back a single stream of traffic, on the local unit, do the following (as appropriate for your particular test); otherwise, if you are looping back multiple streams of traffic, proceed to step 6:

- If you are looping back layer 2 VPLS traffic, specify the far end unit's source MAC address as the destination MAC address for transmitted traffic.
- If you are looping back layer 3 or layer 4 traffic, specify the far end unit's source IP address as the destination IP address for transmitted traffic.
- If you are looping back layer 4 traffic, specify the far end unit's source port number as the destination port for transmitted traffic.

Step6 If you are looping back multiple streams of traffic, source MAC addresses and IP addresses can be specified for *all enabled streams* (on the All Streams tab) or on a *stream-by-stream* basis (on the Ethernet or IP sub-tab for each individual stream).

When looping back multiple streams of layer 4 TCP/UDP traffic, you can specify a unique source service type and port number for each stream, or you can specify the information for one stream, and then copy it to all other streams.

To specify source addresses and ports, on the local unit, do the following:

- If you want to assign a unique source MAC address to each layer 2 stream, be certain to specify **Per Stream** as the Source MAC Mode on the All Streams setup tab, then specify the source MAC addresses on the tabs corresponding to each enabled stream.
- If you want to assign a unique source IP address to each layer 3 stream, be certain to specify **Static-Per Stream** as the Source Type on the All Streams setup tab, then specify the source IP addresses on the tabs corresponding to each enabled stream.
- If you want to assign a unique source port number to each layer 4 stream, specify the port number on the tabs corresponding to each enabled stream.

Step7 On the far end unit, do the following:

a Ensure that automatic traffic generation is not enabled. If it is not disabled, the unit will not respond to the loop up command.

b If you are looping back multiple streams of TCP/UDP traffic, specify a listen port for each enabled stream that matches the destination port in the corresponding stream received from the near end unit.

Step8 On the near end unit, select the Action tab, and then select **Loop Up** to put the far end unit in loop back mode. The following occurs:

– A confirmation message appears in the message bar of the near end unit indicating that the loop back was successful.

– For layer 4 loop backs, if a confirmation message appeared, the ATP listen port (or ports for multiple streams) on the near end are automatically populated.

– If a layer 4 loop back at the far end was successful, and you are looping back traffic using a single stream application, the ATP listen port on the far end is automatically populated.

Step9 On the near end unit, select one of the following:

– **Start Traffic** (if you configured a constant or bursty load).

– **Start Ramp** (if you configured a ramped traffic load).

When the far end unit receives the traffic, it does the following:

– Determines which frames or packets satisfy its filter criteria. Only traffic that satisfies the criteria will be looped back to the near end unit.

– Swaps the destination and source MAC or IP address, and if applicable, port number for every frame or packet it receives.

– Transmits the traffic back to the unit on the near end.

Traffic is transmitted and looped through the unit on the far end (if it passes the far end unit's filter criteria).

To loop down the far end unit

Step1 On the near end unit, select the Action tab, and then select **Stop Traffic** or **Stop Ramp**.

Step2 On the near end unit, select **Loop Down**.

The far end unit is looped down, and a confirmation message appears in the message bar of the near end unit indicating that the loop down was successful.

9

IP Video Testing

This chapter provides information on testing video over IP services. Topics discussed in this chapter include the following:

– “About IP Video testing” on page 202
– “Populating the Address Book” on page 215
– “Specifying interface settings” on page 217
– “Specifying Video settings” on page 217
– “Specifying Ethernet filter settings” on page 217
– “Specifying result threshold settings” on page 219
– “Specifying latency distribution settings” on page 220
– “Specifying IGMP settings” on page 221
– “Joining streams” on page 222
– “Observing physical layer and link statistics” on page 223
– “Observing stream statistics” on page 224
– “Leaving streams” on page 224
– “Basic principles of IP Video testing” on page 225

About IP Video testing

If your instrument is configured and optioned to do so, you can use it to verify the proper installation and configuration of IPTV and IP Video transport service, and then verify that key quality of service (QoS) requirements have been satisfied per a customer's service level agreement (SLA).

The instrument allows you to:

- Automatically discover up to 32 MPTS or 512 SPTS video streams on a circuit.
- Quickly determine whether problems occur at the physical or link layer, on the transport network, or in the video streams themselves by observing the color-coded Summary Status results.
- Determine whether problems are occurring at the video head end, in the transport network, or in the access network by conducting tests at various locations on the network (see Figure 55).
- Validate video flows by configuring the module to emulate a service end point.
- Verify transport network performance of video streams by measuring critical parameters such as bandwidth, packet loss, jitter, and loss distance.
- Analyze multiple streams sent to different end customers and locations to determine whether problems occur in the metro or access segment of the network.

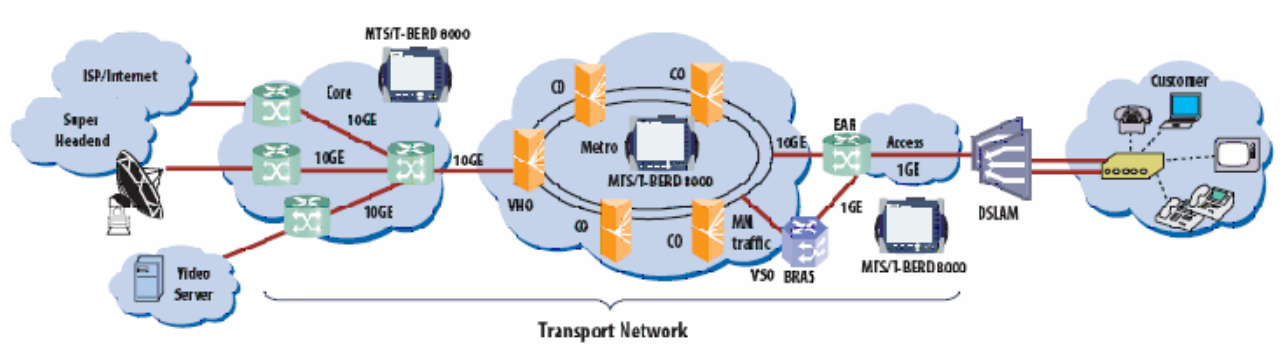


Figure 55 IP Video network architecture

For a brief overview of the key concepts involved in IP Video testing, see "Basic principles of IP Video testing" on page 225.

Understanding MPEG video transport streams

At a minimum, each MPEG video transport stream is comprised of a source and destination IP address, and a UDP port number. They are typically encapsulated within RTP/UDP/IP or UDP/IP streams. If a stream is encapsulated in an RTP stream, the RTP header is also present. If applicable, the required VLAN, VPLS, or Q-in-Q tags or labels are also carried in the stream.

Figure 56 illustrates a typical IPTV encapsulation scheme.

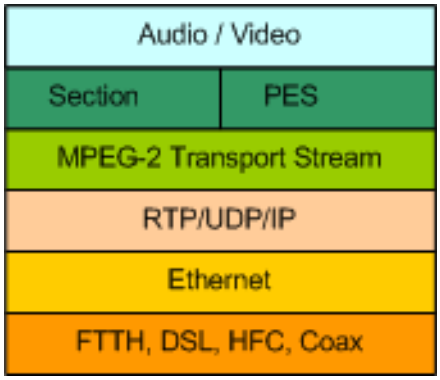


Figure 56 IPTV Encapsulation

Single program transport streams

Single program transport streams (SPTS) carry a single program; therefore, when you run SPTS applications, each of the analyzed streams is carrying one program, and when you observe results in streams view, *program results appear for each stream on a one-to-one basis*.

Multiple program transport streams

Multiple program transport streams (MPTS) carry multiple programs; therefore, when you run MPTS applications, each of the analyzed streams is carrying more than one program, and when you observe results in streams view, *multiple programs appear and can be analyzed for any particular stream*.

Understanding the Explorer and Analyzer applications

The MSAM allows you to quickly determine what is happening on a link by discovering, then observing many MPTS or SPTS transport streams using the Explorer application. If necessary, you can then analyze a single MPTS stream or a subset of SPTS streams in greater detail to troubleshoot issues on the link.

Explorer applications

The Explorer applications allow you to discover and then monitor up to 32 MPTS or 512 SPTS streams, and observe key results such as the MPEG status, the number of programs carried in the stream, the layer 1 bandwidth utilized by the stream (in Mbps), packet loss, and packet jitter measurements. When running an Explorer application, you can establish thresholds for declaring key errors, such as IP jitter and packet loss.

Analyzer applications

The Analyzer applications allow you to monitor a single MPTS stream or 16 SPTS streams, observe comprehensive transport layer and MPEG-2 layer results, and observe aggregate physical layer and link statistics for the stream or streams. When running an Analyzer application, you can establish detailed thresholds for declaring a variety of errors, including:

– Continuity errors

- PCR Jitter
- Synchronization errors
- Transport (TEI) errors
- PAT, PMT and PID errors
- MDI delay factor and media loss rate (if optioned)
- Packet jitter, loss distance, and loss periods
- Packet Loss

Understanding MSTV

Microsoft media room television (MSTV) is Microsoft's proprietary IPTV. It is a distributed operating system that runs both on the servers and on the STBs. It performs end-to-end configuration, provisions the video servers, links the electronic program guide (EPG) with the content, acts as a boot server for the STB and ensures that all STBs run compatible software. MSTV Architecture contains a number of servers, running on Microsoft platforms used to provide content storage and delivery in a service provider's network. MSTV streams are almost always VBR streams.

Acquisition server (A-Server) performs live content acquisition from various local and terrestrial sources for linear broadcast TV. A -Server packetize it over RTP and send it to all D-server and STBs listening to the same sources.

Distribution servers (D-servers) are used to distribute frequently used content from various points of presence in the provider's network for faster access and to minimize channel switching time. D-Server serves the STB clients with both R-UDP and ICC, which are transmitted as unicast packets of TS/RTP/UDP. Lost packets are also restored between A and D server with R-UDP unicast or multicast packets.

STBs are customer premises equipment interfaced with the TV which also run Microsoft proprietary software. For a channel change, the STB sends ICCIGMP join request to the D-server and D-server sends a response back, followed by a short unicast burst of traffic to enable the channel change.

Instant Channel Change (ICC)

Unlike channel switching on cable TV, where changes are "instant", inherent switching and routing delays in an IP network cause channel switches to be visibly slower (one to two seconds). To eliminate the channel change delay inherent in digital cable, satellite, and IPTV networks set-top-boxes support Microsoft Instant Channel Change (ICC) capability used to implement very fast channel change.

Microsoft uses a combination of short unicast burst of data (starting with an MPEG "I" frame) at a 20-30% higher bitrate than normal at the beginning of channel tuning from the STB to the D-Servers, Begins with I frame so that playback can begin immediately. Fills the STB buffer. After the buffer is full it joins the multicast stream. The first request implements ICC by accelerating video for the first seconds, followed by 'normal' video flow.

Channel change time, also known as Zap time, is an important metric for IPTV QOS. Zap time refers to the channel change delay, or how quickly and reliably the user can change the channel. It is the time between sending of channel leave request and receiving of first video stream data for the new, just joined video stream.

Microsoft R-UDP

MSTV uses R-UDP protocol for IPTV service delivery over multicast networks. This is Microsoft proprietary protocol. It focuses on replacing lost packets as reported by a STB. Retries between Dserver and STB is unicast. The source listens on a IP or UPD port for the retries.The STB makes requests for the lost packets. The Dserver responds with lost packets as unicast packets of TS/RTP/UDP. The Dserver uses the overhead bandwidth allocated over the max bit rate to server the additional packets.The lost packets are reported to the DServer in the format of the starting sequence number of the hole, followed by the number of packets in this hole.

Features and capabilities

Features and capabilities of the Dual Module Carrier, Transport Module, and MSAM include the following when testing IP Video service:

- Address book—If you need to monitor specific streams on a regular basis, you can add them to the address book to expedite the setup process for future tests. You can also import addresses from and export addresses to a USB key. After adding them to the address book, you can quickly select them when joining streams using IGMP requests. For details, see “Populating the Address Book” on page 215.
- Timed tests and event log—You can schedule tests to run for a specific period of time, and archive all events to a log for review at a later time. This is useful when evaluating sporadic packet loss on a circuit, or correlating PCR jitter to instances of overall packet jitter. For details on timed tests, see the Getting Started manual that shipped with your instrument or upgrade. For details on the Event log, see “Event Log results” on page 414 of Chapter 13 “Test Results”.
- IGMP Version 2 or Version 3—You can optionally use Version 2 or Version 3 of IGMP to request specific video streams when testing.
- Traffic filters—You can optionally filter monitored streams for non-tagged, VLAN, Q-in-Q, or VPLS traffic.
- Result thresholds—When running Explorer applications, you can monitor transport streams for packet loss and packet jitter, and either use the default thresholds for declaring QoS alarms for either condition, or establish your own thresholds. Additional thresholds are available when running Analyzer applications.
- Bandwidth utilization—You can determine the bandwidth utilized for each transport stream, and then verify that error free traffic is received for each stream.
- TR 101 290 First Priority results—You can observe the first priority results recommended in ETSI TR 101, such as transport stream synchronization loss, and continuity, PAT, PMT, and PID error counts.
- Detailed result analysis—You can observe detailed information for a subset of transport streams using the Analyzer application, and then compare results for the streams to determine if errors are due to the same root cause.
- Identification of stream type. The instrument analyzes the stream to identify whether it is a CBR or VBR stream. The available results vary depending on the stream type.
- MSTV. Support for Microsoft IP TV in SPTS Analyzer mode. MSTV can monitor up to 16 multi-cast streams.

Understanding the graphical user interface

When you configure your module for testing, the main screen provides three result buttons that allow you to display physical/link quality results, transport streams quality results, and video streams quality results. Setup tabs are provided that allow you to specify filter criteria for monitored

streams and establish thresholds for declaring certain errors such as packet loss or packet jitter. If you intend to actively request specific streams using IGMP, you can also specify settings that control the requests.

Action buttons

When running IP Video applications, buttons appear at the bottom of the Main screen that allow you to select an SFP or specify the wavelength for an optical connector (if applicable), turn the laser on or off, and, if you are using IGMP, actively join or leave specific transport streams.

Restart button

When running IP Video applications, if streams are dropped during the course of your test, they will continue to appear on your display, but the current bandwidth measurement (`Total Util %, Cur`) will be zero. If this occurs, you can press the Restart button to refresh the display and show all *currently analyzed streams*. The dropped streams will be cleared from the display.

Understanding the LED panel

When you select an IP Video application, LEDs appear under the result window on the Main screen (see Figure 57).



Figure 57 IP Video LEDs

The LEDs allow you to quickly determine whether a signal is present, synchronization has been acquired, and whether or not the link is active. LEDs also indicate whether or not frames or packets are detected on the link.

Understanding IP Video test results

IP video results are available that allow you to verify the quality of the physical layer, the link, the transport quality of video streams, and the quality of the video streams and programs themselves. Figure 58 illustrates the buttons used to verify the quality of service in each area.

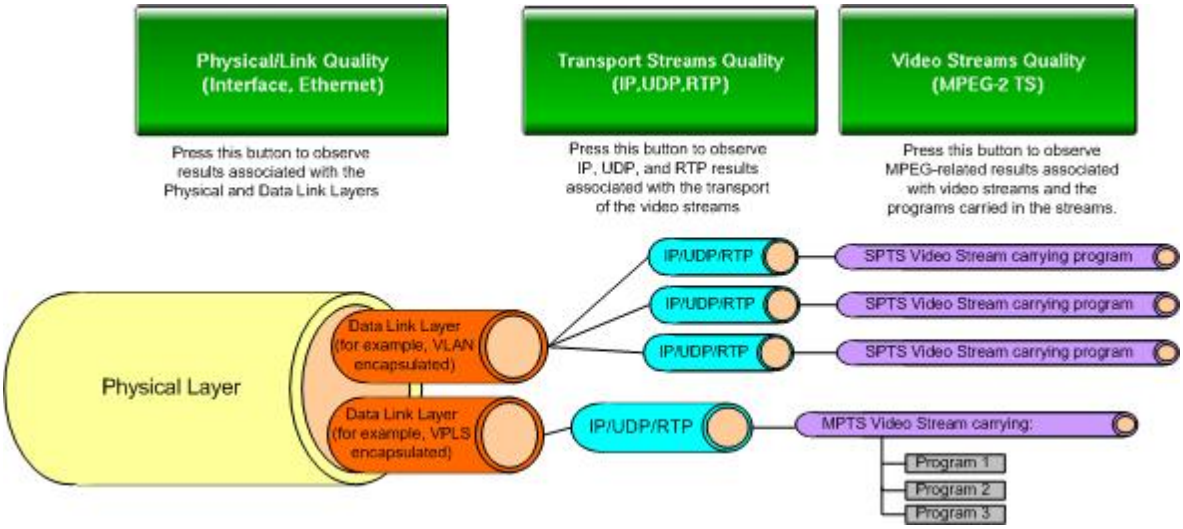


Figure 58 IP Video Quality Buttons

Layered view: Quality Layer Buttons

The layered view appears on the Main screen the first time you launch an IP Video application. Color coded quality buttons appear which immediately indicate the current and historical status of the physical layer and link, the transport of the video streams (using IP, UDP, and RTP), and the video streams and programs themselves. Figure 59 illustrates the view when all results are OK and there is no history of errors at any layer.

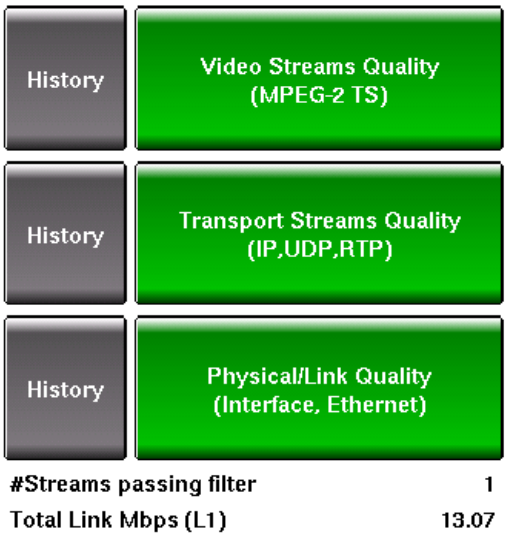


Figure 59 Layered View - All Results OK

Physical/Link Quality (Interface, Ethernet)—This button displays aggregate results (such as the bandwidth utilization, interface (layer 1) and Ethernet (layer 2) errors for the link.

Transport Quality (IP, UDP, RTP)—This button displays test results for each monitored IP, UDP, or RTP traffic stream.

Video Streams Quality (MPEG-2 TS)—This button displays test results for each monitored MPEG-2 video transport stream.

After streams are discovered on the link, a count of the number of streams passing the filter criteria, and the total layer 1 bandwidth utilized and appears under the buttons.

Navigation Tip:

You can always return to the layered view by setting the results group to **Summary**, and the category to **Status**.

Layered View: Button Colors

Figure 60 illustrates the view when there are errors at the transport stream layer and there is a history of errors at both the transport stream and video stream layer. The Video Streams Quality button indicates that it can not provide results for video streams because there are errors with the underlying transport streams (`Lower Layers Errored`). No errors have occurred at the physical/link layer.

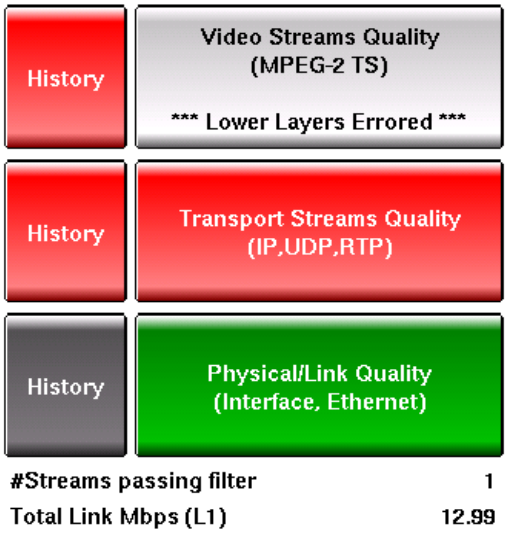


Figure 60 Layered View - Errored Transport Streams

Table 17 explains each of the colors used for the current and history buttons.

Table 17 Current and History Button Colors

Color	Current	History[a]
Green	Indicates that all results are OK for that particular quality group. For an example, see Figure 59 on page 207.	N/A

Table 17 Current and History Button Colors (Continued)

Color	Current	History[a]
Yellow	Indicates that at least one result at that particular layer triggered a minor alarm or error based on the established thresholds.	Indicates that at least one result occurred within the last test interval that triggered a minor alarm or error based on the established thresholds. For an example, see Figure 62 on page 210.
Red	Indicates that at least one result at that particular layer triggered a major alarm or error based on the established thresholds.	Indicates that at least one result triggered a major alarm or error based on the established thresholds within the last test interval. For an example, see Figure 63 on page 211.
Light Gray	Indicates that results are not available because there is an issue at a lower level that prevents your unit from determining the status for that particular quality group. For an example, see Figure 63 on page 211. If a button is gray, evaluate the test results for the lower layer to determine the nature of the problem.	N/A
Dark Gray	Indicates that your unit can not detect the signal, packets, or streams required to provide the status for the quality layer. A message appears on the button stating what could not be detected (No Signal, No IP Streams, or No MPEG-2 Streams). For an example, see Figure 61 on page 210.	Indicates that nothing has occurred within the last test interval to trigger a yellow or red state.

a. If errors are intermittent, the large quality button (indicating the current state of the results) will be green, but the associated history button will be red or yellow. This is due to the five second refresh rate of your unit. Therefore, it is important to check the state of the history button periodically during the course of your test to verify that intermittent errors are not occurring.

Figure 61 illustrates the layered view when no IP or MPEG-2 streams are detected, and there is a history of errors at the transport and video stream layers.

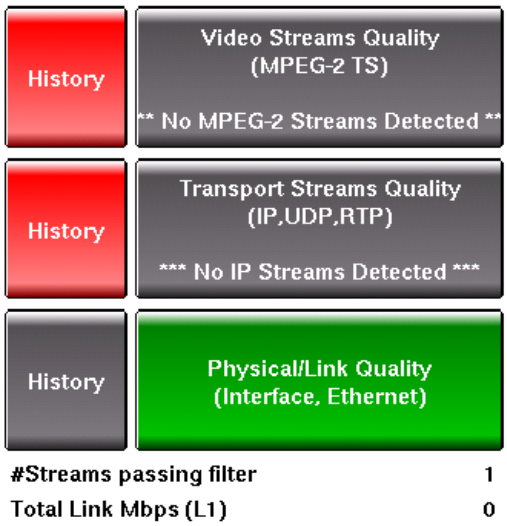


Figure 61 Layered View: No IP or MPEG-2 streams detected

Figure 62 illustrates the layered view when errors occurred at the transport layer, and there is a history of warnings at the video stream layer.

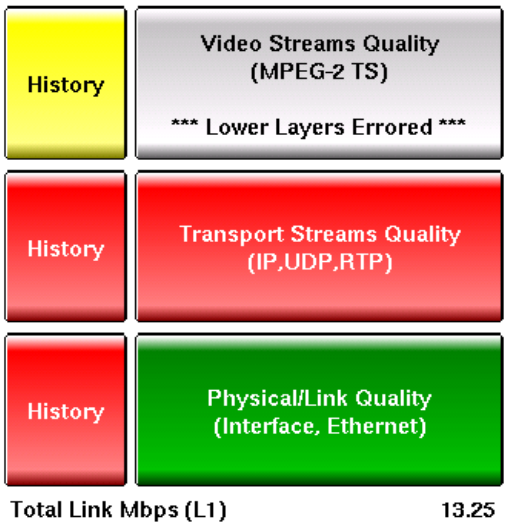


Figure 62 Layered View: History of Warnings at Video Stream Layer

Streams view

The streams view appears by default after you select the **Transport Streams Quality** or **Video Streams Quality** button.

– When you press the **Transport Streams Quality** button, all monitored streams are listed.
– If you press the **Video Streams Quality** button while running an MPTS application, all programs for each monitored MPTS appear.
– If you press the **Video Streams Quality** button while running an SPTS application, monitored SPTS streams appear (see Figure 63).

To optimize the number of results that appear on your display, the result windows appear in the Full Size view by default when you run IP Video applications.



Figure 63 Video Results: Streams View (MPTS Transport Stream, Explorer application)

Stream status icons

Table 18 explains each of the icons that may appear to the left of the monitored streams.

Table 18 Stream Status Icons

Icon	Indicates
	No errors have been detected on the monitored stream.
	One or more errors satisfying the alarm threshold have been detected on the monitored stream. Errored results also appear with a red background. If you see a stream with a red exclamation mark, but no results appear in red, one of the hidden results is errored. If this occurs, select the **Columns** button, and then press **Select all** to show all of the results available for the stream. Scroll to the right of the results display until you locate the errored result (or results).
	One or more errors satisfying the warning threshold have been detected on the monitored stream. Errored results also appear with a yellow background.

Observing streams using the Explorer Application

You can do the following when running an Explorer application:

– Observe a list of transport traffic streams or video streams by pressing the **Transport Streams Quality** or **Video Streams Quality** button provided in the layered view to observe a list of transport traffic streams or video streams.

– Observe transport and video streams simultaneously by selecting the current result group button (**All Streams Video** or **All Streams Transport**), and then selecting **All Streams Complete**.

– Evaluate certain streams more thoroughly (using the Analyzer application) by selecting the streams, and then pressing **Launch Analyzer** directly from the streams display. It is not necessary to launch the application from the Test menu. If you are analyzing streams on an optical circuit, you'll need to turn the laser on again after the Analyzer application launches. If you originally joined the streams via an IGMP request, you must re-join them. See "Joining streams" on page 222.

  If you have streams displayed in multiple result windows, you can only launch one instance of the Analyzer application. You can not launch multiple instances of the Analyzer from different windows.

Observing streams using the Analyzer Application

You can launch the Analyzer application using either method below:

– Via the Test Menu, which provides Analyzer applications for SPTS and MPTS streams.

– From an Explorer application, if you want to analyze a subset of streams in greater detail. A Launch Analyzer action button appears at the bottom of the streams result display, allowing you to launch the application for selected streams immediately (without returning to the Main screen).

You can do the following when running an Analyzer application:

– Press the **Transport Streams Quality** or **Video Streams Quality** button provided in the layered view to observe a list of transport traffic streams or video streams.

– If you would like to observe transport traffic streams and video streams simultaneously, select the current result group button (**All Streams Video** or **All Streams Transport**), and then select **All Streams Complete**.

– If you would like to observe results for a particular stream, select the current result group button, and then select the group corresponding to the stream number (for example, **Stream 3**). If the stream is named, its name (for example, ESPN or CNN) appears in the group list instead of a stream number.

– If you launched the Analyzer application from the Explorer application, after you analyze the streams that were discovered by the Explorer application (which were transferred to the Analyzer application), you can press the **Rescan Streams** soft key to rescan the link and discover the current streams meeting your filter criteria. Discovered streams will not be restricted to those that were previously discovered using the Explorer application.



Navigation Tip:

You can always return to the streams view by setting the results group to **All Streams (Complete)**, **All Streams Video**, or **All Streams Transport**.

Restart Warning:

If you launch an Explorer or Analyzer application from the Test Menu, pressing **Restart** clears all discovered streams from your display, and your unit rescans the circuit and discovers streams that are currently on the circuit. Therefore, if you are in the process of analyzing results for a particular stream, *do not press **Restart***.

If you launch the Analyzer application from an Explorer application (using the **Launch Analyzer** button), pressing **Restart** will only clear your test results; it will not rescan the circuit for new streams. The **Rescan Streams** soft key is used to discover new streams.

Static and dynamic test results

When streams (and programs) are first discovered, values for certain results are determined, displayed, and then remain ***static***. These values remain the same until you "discover" streams or programs again. All other dynamic results are refreshed every five seconds.

Table 19 lists static results for each stream when running the Explorer or Analyzer applications.

Table 19 Static IP Video Stream Test Results

Result	Explorer?	Analyzer?
IPv4 Source Address	Yes	Yes
IPv4 Destination Address	Yes	Yes
UDP Dest Port	Yes	Yes
UDP Source Port	Yes	Yes
RTP Present	Yes	Yes
VLAN ID	Yes	Yes
VLAN Priority	Yes	Yes
SVLAN ID	Yes	Yes
SVLAN Priority	Yes	Yes
VC Label (VPLS)	Yes	Yes
Tunnel Label (VPLS)	Yes	Yes
Number of Programs	Yes	Yes
Transport Stream ID	No	Yes

Table 20 lists static results for each program when running an Analyzer application.

Table 20 Static IP Video Test Results - Analyzed Programs

Result
PMT PID
Program Number
of PIDs
PID ID
PID Types (such as Audio, Video, Other)

Navigating the results display

When navigating through the IP Video results, consider the following:

– When you launch an application for the first time, the Summary group and Status category appear. This is also referred to as the “layered” view (see “Layered view: Quality Layer Buttons” on page 207).
– When you launch applications subsequent times, the result view that was displayed the last time you ended a test appears. For example, if the All Streams Video results were displayed the last time you ran the MPTS Explorer application, the next time you launch the application, the All Streams Video results will appear (see Figure 63 on page 211).
– Use the Result Group button to switch between the Summary, Physical/Link, All Streams (Complete), All Streams Video, and All Streams Transport groups.
– When observing results in the Physical/Link group, Stats and AutoNeg Status categories are available. Use the category button to switch categories.
– When observing results in one of the All Streams groups, the only category that is available is the All category.
– If you’d like to observe more detailed information for a particular stream, you can select the stream, and then press **Stream Details**. Some results are only available when viewing detailed results for a particular stream. For example, if you are analyzing video streams carried on a VPLS network, you must press **Stream Details** to see the VLAN, SVLAN, Tunnel, and Virtual Channel (VC) for the stream.
– If you’d like to observe detailed results for a particular stream or program, tap twice quickly (double-click) on the stream or program. For example, if you are analyzing SPTS, double clicking on the first stream displays the bandwidth utilized for the stream or program, PCR jitter measurements, and counts for a variety of errors.
– If an up or down arrow appears in a column label, you can tap on the label to sort the streams in ascending or descending order.

Customizing the results display

Some categories provide so much information you may need to scroll to the right significantly to observe a particular result. In other instances, you may be monitoring a large number of transport or MPEG-2 streams, which forces you to scroll up and down to observe results for each analyzed stream.

To focus on a particular subset of results (and minimize scrolling), you can specify which result columns appear on your display, and hide those that do not apply to your test. For example, if each of the streams you are analyzing is named, and the circuit is not configured for VPLS traffic, you may choose to hide the IP Address, Tunnel, and VC (virtual channel) columns since they are not necessary when evaluating your results.

To reduce the number of streams displayed, you can optionally show only errored streams (rather than all monitored streams).

IP Video test applications

This release of the instrument supports the IP Video test applications for the interfaces listed in Table 21.

Table 21 IP Video test applications

Application	10/100/1000	100M Optical	1 GigE Optical	10 GigE LAN	10 GigE WAN
MPTS Explorer	√	√	√	√	N/A
SPTS Explorer	√	√	√	√	N/A
MPTS Analyzer	√	√	√	√	N/A
SPTS Analyzer	√	√	√	√	N/A

Populating the Address Book

The Dual Module Carrier, Transport Module, and MSAM provides an Address Book which you can populate with the streams that you know you intend to request and monitor on a regular basis. When running MPTS applications, you can also add and name specific programs carried in each stream.

After you store streams and programs in the address book, you can join them using the **Join Streams** button provided on the Main screen.

Adding streams

To add streams to the address book

Step1 If you haven't already done so, launch an IP Video application. For a list of applications, see Table 21 on page 215.

Step2 Press the **Address Book** soft key.

Step3 Under New Entry, specify the following:

a If the stream is identified using a combination of source IP address and destination address, in Source IP, enter the source address for the stream; otherwise, accept the default value of 0.0.0.0 (which indicates that streams with any source address carrying the specified destination address will be added).

A source IP address is only required if you are issuing requests using IGMPv3.

b In Dest. IP, specify the destination address carried in the stream. The destination IP address is required.

c Optional. If you are running an MPTS Analyzer application, and you want to specify the program ID carried in the program mapping table (PMT) for the stream, in **PMT PID**, enter the PID. If you intend to name the stream, you must specify the PID (to distinguish the program from other programs carried in the stream).

d In **Name**, type the name you want to use to identify the stream or program.

Step4 Select **Add Entry**.

The stream is added to the address book, and it appears in the streams list. Delete and Delete All buttons are provided if you need to remove streams from the book.

Updating stream data

After you add a stream, you can update the name, source IP address, destination IP address, and if applicable, PID by selecting the corresponding data on your touch screen.

To update stream data

Step1 Select the data you want to update (Name, Source IP, Destination IP, or PMT PID).

A keypad appears.

Step2 Type the new name, address, or PID, and then select OK.

The data is updated.

Importing or exporting streams

You can store a list of streams as a CSV file on a USB key, and then import them into the address book. You can also export address book data to a USB key, and then load it onto another unit.

To import streams

Step1 If you haven't already done so, launch an IP Video application. For a list of applications, see Table 21 on page 215.

Step2 Press the **Address Book** soft key.

Step3 Insert the key with the CSV file into a USB slot on your unit.

The unit beeps to indicate that it recognized the key.

Step4 To import stream entries, do the following:

- **a** Select **Import**. The Import Entries From USB dialog box appears.
- **b** Select the .csv file with the entries that you want to import, and then select **Import Entries**.

Streams are imported, and appear on the dialog box.

Step5 To export stream entries, do the following:

- **a** Select **Export**. The Export Entries To USB dialog box appears.
- **b** Type a file name for the CSV file that will contain the exported stream entries, or accept the default file name (IPTV_Address_Book_YYYY-MM-DD, where YYYY represents the current year, MM represents the month, and DD represents the day). If you enter your own filename, you do not need to type the .csv extension.
- **c** Select **Export Entries**.

Streams are exported to the USB key.

Stream entries are imported or exported.



TIP: SORTING PHONE BOOK ENTRIES

You can easily sort the entries in ascending or descending order using the data provided. For example, to sort the entries by name, select the heading for the Name column. To sort the entries in descending order by destination IP address, select the Destination IP heading. Selecting a heading a second time reverses the order.

Specifying interface settings

Before monitoring IP Video traffic on an optical circuit, you can specify interface settings which:

– Indicate which SFP jack you are using (if your unit is equipped with SFP jacks).
– Specify the transmitted wavelength (if your unit is equipped with 850 nm, 1310 nm, and 1550 nm connectors).
– Allow your unit to communicate with another Ethernet device (when requesting video traffic using IGMP).

For details on the various connectors used to connect to the circuit, refer to the printed Getting Started User's Manual that shipped with your unit. For details on specifying the information required to establish a link to another device, see "Specifying interface settings" on page 46 of Chapter 4 "Ethernet and IP Testing".

Specifying Video settings

After specifying interface settings, specify the Video settings. These settings are only available in SPTS Analyzer applications.

To specify video settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **Video** tab.

Step3 Specify the **Protocol Mode**: IPTV (typical IPTV) or MSTV (Microsoft proprietary IPTV).

The video settings are specified.

Specifying Ethernet filter settings

Before monitoring video traffic, you can specify settings that determine which traffic passes through the filter for analysis. For example, you can set up the filter to observe multicast traffic carried on a specific VLAN, or unicast and multicast traffic carried on a particular VPLS tunnel, or traffic for a specific STB.



NOTE:

If you are joining specific streams using IGMP requests, be certain to configure the filter using the same encapsulation criteria to ensure that the streams pass through the filter for analysis. For details, see "Joining streams" on page 222.

To filter received traffic

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **Ethernet Filter** tab.

Step3 If you do not want to analyze video streams on a VPLS circuit, skip this step and proceed to step 4.

If you want to analyze video streams on a VPLS circuit, specify the following filter settings:

Setting	Specify
VPLS Enabled	Yes
Tunnel ID Filter	If you want to analyze video streams carried on a specific tunnel, select **Yes**; otherwise, to analyze streams carried on any tunnel, select **Don't Care**.
Tunnel ID (Tunnel ID Filter is Yes)	Enter the ID for the tunnel carrying the video streams that you want to analyze.
VC ID Filter	If you want to analyze video streams carried on a specific virtual circuit, select **Yes**; otherwise, to analyze streams carried on any circuit, select **Don't Care**.
VC ID	Enter the ID for the virtual circuit carrying the video streams that you want to analyze.

Step4 In Encapsulation, specify the type of traffic you want to analyze:

Encapsulation	Settings
None, VLAN, or Q-in-Q	No additional settings required. Only unencapsulated, VLAN-tagged, or Q-in-Q tagged traffic will pass through the filter for analysis. VPLS traffic will not be analyzed.
None	No additional settings required. Only unencapsulated traffic will pass through the filter for analysis. VPLS traffic will not be analyzed.
VLAN	Specify VLAN ID If you want to analyze traffic carried on a specific VLAN, select **Yes**; otherwise, to analyze traffic on multiple VLANs, select **Don't Care**.
	VLAN ID (Specify VLAN ID must be Yes) Specify the ID of the VLAN carrying the traffic you want to analyze.
Q-in-Q	Specify CVLAN ID If you want to analyze traffic on a specific customer or service provider VLAN, select **Yes**; otherwise, to analyze traffic on multiple VLANs, select **Don't Care**.
	CVLAN ID (Specify CVLAN ID must be Yes) Specify the ID of the customer VLAN carrying the traffic you want to analyze.
	SVLAN ID (Specify CVLAN ID must be Yes) Specify the ID of the service provider VLAN carrying the traffic you want to analyze.

Step5 In Traffic Type, specify whether you want to analyze **Multicast** traffic (traffic sent to a variety of destinations), or **Multicast & Unicast** traffic (traffic sent to a variety of destinations, or to a single destination).

The settings are specified to filter traffic for analysis.

Specifying result threshold settings

Before analyzing traffic, you can specify settings that control how your unit interprets a variety of test results. Thresholds for declaring that certain results are in an alarm state (and reported in red on your results display), and whether they are *approaching* an alarm state (and reported in yellow) are available. Red results (results in an alarm state) are also reported in the Event Log.

For example, when configuring an Explorer application, you can indicate that if more than two packets are lost during a test interval (5 seconds), the packet loss result (and any associated result buttons) should appear in red. You can also indicate that if more than one packet is lost, the result and buttons should appear in yellow (to serve as a warning that something may be wrong).

When configuring Analyzer applications, you can also indicate when certain errors, such as period errors or distance errors should be declared.

The test interval used to calculate alarm results varies depending on the type of result (see Table 22). Each test interval is treated as a separate time slot.

Table 22 Alarm Test Intervals

Result	Test Interval	Explorer Application	Analyzer Application
Packet Loss	5 seconds	Yes	Yes
Continuity Counter Errors	5 seconds	No	Yes
MDI Media Loss Rate	5 seconds	No	Yes
Sync Errors	5 seconds	No	Yes
PAT/PMT Errors	5 seconds	No	Yes
Transport Errors (TEI)	5 seconds	No	Yes
PID Errors	5 seconds	No	Yes
Packet Jitter (ms)	1 second	Yes	Yes
MDI Delay Factor	1 second	No	Yes
MDI Media Loss Rate	1 second	No	Yes

To specify result threshold settings

Step1 If you haven't already done so, use the Test Menu to select the IP Video application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **Result Thresholds** tab.

Step3 Under QoS Alarm Thresholds, for each result listed, specify the following:

- In **Raise alarm if above**, specify the threshold for displaying the result (and any associated buttons) in red.
- In **Warn if at least**, specify the threshold for displaying the result (and any associated buttons) in yellow.

If you are configuring an Explorer application, or if the streams you are analyzing are not encapsulated using RTP, the thresholds are specified. You do not need to proceed to step 4.

Step4 If you are configuring an Analyzer application, and the analyzed streams are carried in RTP, specify the following under QoS Error Thresholds:

– **Period Error - Loss Period must exceed**. Enter the threshold for declaring a Period Error. The threshold represents the number of packets ***lost sequentially*** before a Period Error is declared. The number of sequentially lost packets constitutes the “Loss Period”.

– **Distance Error - Distance between periods must fall below**. Enter the threshold for declaring a Distance Error. The threshold represents the minimum number of packets that must be received in between declared Loss Periods to constitute ***an acceptable distance between errors***. If the number of received packets between Loss Periods falls below the threshold, a Distance Error is declared. Essentially, the specified number of packets constitutes the “distance”.

The result thresholds are specified. Alarms, warnings, errors, and the Event Log will be handled according to your settings.

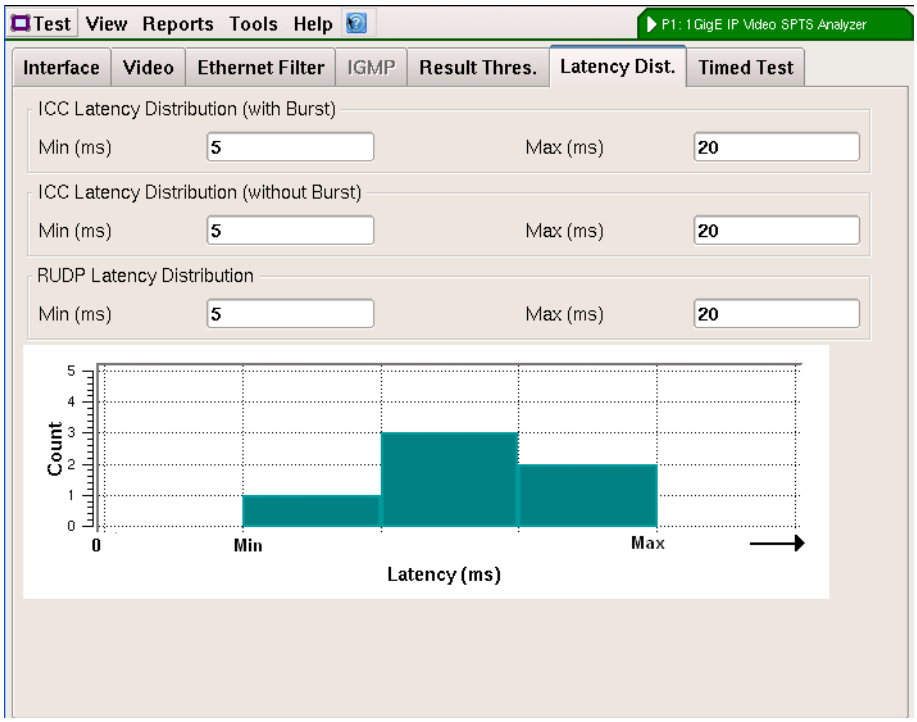
Specifying latency distribution settings

If you are testing Mirosoft IPTV streams (selected MSTV on the Video setup screen), the latency distribution settings are available.

To specify latency distribution settings

Step1 If you haven’t already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **Latency Dist.** tab.



Step3 Specify the following:

Setting	Description
ICC Latency Distribution (with Burst)	Specify the minimum and maximum amount of time, in milliseconds, of an MSTV ICC request message to the first unicast media packet.
ICC Latency Distribution (without Burst)	Specify the minimum and maximum amount of time, in milliseconds, of an MSTV ICC request message to the first multicast media packet.
RUDP Latency Distribution	Specify the minimum and maximum amount of time, in milliseconds, of an MSTV RUDP request message to the first unicast retry media packet.

The latency distribution settings are specified.

Specifying IGMP settings

Before testing, you can set up your unit to emulate a downstream IGMP client, and then actively request video streams from an IGMP router. To do so, you specify the version of IGMP to use (Version 2 or 3), and the source IP address, subnet mask, and default gateway for the unit. You can also optionally use DHCP to assign the IP address data for you.

After specifying the IP address data, you can specify a user-defined source MAC address for your unit, or you can use the factory assigned MAC address Finally, you should specify the frame format used on the network to ensure that streams are not dropped during the course of your test. You can optionally encapsulate the requests in VLAN or Q-in-Q tagged Ethernet frames. If you do so, you must specify the associated VLAN IDs and priorities.

If you are issuing the requests using IGMP Version 2, you can specify durations to wait before retrying requests for a single stream or multiple streams.



IGMP WARNING:

Be certain to configure IGMP on your unit before using it to join streams. If you change any setting on the IGMP setup screen after joining streams, the unit will *automatically leave all currently joined streams*.

To specify your unit's IGMP settings

Step1 If you haven't already done so, use the Test Menu to select the IP Video application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **IGMP** tab.

Step3 Under Customize IGMP Requests, in Format, select **IGMP v2** or **IGMP v3**.

Step4 If no reply is received to in response to a request, your unit will wait 120 seconds before issuing another join request for a single stream and 50 milliseconds between consecutive stream requests.

If you are using **IGMP v3**, your unit will wait for a response for the default intervals before issuing another request; proceed to step 5.

If you selected **IGMP v2**, and you would like to change the default intervals, select the appropriate field, and then specify the interval.

Step5 In **Source IP Type**, indicate whether you are using a static IP address, or whether you want to use DHCP to assign the address for you. If you use a static address, specify the Source IP address, Subnet Mask, and Default Gateway carried by the requests.

Step6 Specify the **Source MAC** address type (**Factory Default** or **User Defined**). If you select User Defined, specify the address.

Step7 In **Ethernet Frame Type**, indicate whether the requests are made using DIX or 802.3 frames. Be certain to enter the same format used by switches on the circuit you are monitoring.

Step8 In **Encapsulation**, select **None**, **VLAN**, or **Q-in-Q**. If you select VLAN or Q-in-Q, specify the required encapsulation settings. For details on the settings, refer to "Configuring VLAN tagged traffic" on page 54 and "Configuring Q-in-Q traffic" on page 55 of Chapter 4 "Ethernet and IP Testing".

Step9 If you specified VLAN or Q-in-Q as your encapsulation setting, to ensure that traffic passes through the filter for analysis, select the **Ethernet Filter** tab, and then specify the same encapsulation settings.

The settings are specified. You are ready to join streams (see "Joining streams" on page 222).

Joining streams

To join a particular stream (or streams), you press the **Join Streams** button on the Main screen, and then either select the stream from the address book, or specify the address (or addresses) for the stream that you want to join manually. Table 23 lists the number of streams you can join when running each of the IP Video applications.

Table 23 Maximum number of streams analyzed

Application	SPTS	MPTS
Explorer	512	32
Analyzer	16	1

After your instrument discovers streams for analysis, you can only actively join streams up to the maximum number supported. For example, if you are running an MPTS Explorer application, and your instrument discovers 30 video streams, you can only actively join and then analyze two additional streams.

Although you can add streams as you need them on the Join Streams screen, if you'd like to name the stream or name a PMT PID for a specific program for a stream, you must use the Address Book soft key provided on the Main screen. For details, see "Populating the Address Book" on page 215.

To join streams

Step1 If you haven't already done so, use the Test Menu to select the IP Video application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 On the Main screen, select the **Join Streams** button.

The Join Streams screen appears.

Step3 For each of the streams you want to join, do one of the following:

If....	Do this ...
The stream appears in the Address Book	Tap on the stream, and then press **Select**. The stream appears under Selected Streams.
You are using IGMP v2, and the stream does not appear in the Address Book	Tap the Dest. IP field, and then use the keypad to enter the destination IP address for the stream.
You are using IGMP v3, and the stream does not appear in the Address Book	– If you want to request the stream using just the destination IP address, accept the default source IP address (0.0.0.0), and then enter the destination IP address. – If you want to request the stream using a source IP address and destination IP address, tap each field to enter the addresses.

The streams are selected, and appear under **Selected Streams**.

Step4 After selecting the streams, press **Join Streams**.

You are returned to the Main screen. Your unit issues IGMP requests to join the streams, and messages concerning the status of the request appear in the Message bar at the top of the screen.

Step5 Select the **All Streams Complete**, **All Streams Transport** or **All Streams Video** result group.

Results for the requested streams appear.

If, after waiting for 5 seconds, streams do not appear, press **Setup**, and then verify that you have specified the correct Ethernet Filter and IGMP settings (see “Specifying Ethernet filter settings” on page 217 and “Specifying IGMP settings” on page 221).

Observing physical layer and link statistics

When monitoring video streams, you can quickly verify the state of the physical layer and the link by observing the Physical/Link Quality button. If green, all results are OK at these two layers.

If the button is yellow or red, you must investigate and resolve the problem before evaluating transport and video stream results.

To observe physical layer and link statistics

Step1 If you haven’t already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 On the Main screen, press the **Physical/Link Quality** button.

The Physical/Link result group appears, showing aggregate statistics for the physical layer and the link. For example, the total number of Sync Loss Seconds or Rx IGMP frames are provided in the Stats category.

Step3 If you want to observe results associated with the auto-negotiation of the link, set the result category to **AutoNeg Status**.

The physical layer and link statistics were displayed. For descriptions of each of the results, refer to “CPRI/OBSAI test results” on page 341 of Chapter 13 “Test Results”.

Observing stream statistics

You can quickly verify the state of monitored transport and video streams by observing the colors of the Transport Streams Quality and Video Streams Quality buttons. Pressing the buttons allows you to observe results at each layer in more detail.

To observe stream statistics

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 21 on page 215 for a list of applications.

Step2 On the Main screen, press one of the buttons:

- **Transport Streams Quality**. The All Streams Transport result group appears.
- **Video Streams Quality**. The All Streams Video result group appears.

Step3 Use the scroll bars to browse through the monitored streams. To customize your results, you can optionally do the following:

- If you are monitoring a large number of streams, and you want to focus only on errored streams, select **Show only errored streams**.
- If too many results appear for the streams, or if the results you expected to see do not appear, select **Columns...**, and then clear the check box next to the results you want to remove, or select the check box next to the results you want to add to the display. Press **Ok** to return to the result display.
- If you are running an Explorer application, and there are streams that you want to analyze in more detail, select the **Analyze** check box (to the left of the stream results), and then press **Launch Analyzer**.

  The SPTS or MPTS analyzer application is launched. If you are monitoring streams on an optical circuit, turn the laser back on. If you originally joined the streams using an IGMP request, re-join the streams (see "Joining streams" on page 222).

  A more detailed set of results appears for the analyzed streams.

You are observing stream statistics.

Leaving streams

If you actively joined streams using IGMP requests, when you are done testing, you should leave them.

To leave a stream

Step1 On the Main screen, press **Leave Streams ...**.

The Leave Streams dialog box appears, listing each of the streams you actively joined.

Step2 Select each of the streams you want to leave, and then press **Leave Streams**.

You are returned to the Main screen. Your unit issues IGMP requests to leave the streams, and messages concerning the status of the request appear in the Message bar at the top of the screen.

Basic principles of IP Video testing

This section presents some of the basic principles behind IP Video testing. For a comprehensive discussion of IP Video troubleshooting, please contact Customer Care for a copy of the *JDSU Triple Play Service Deployment Guide*.

IP Video network architecture

Figure 55 on page 202 illustrates a typical IP Video network. When troubleshooting IP video service, the first step is to determine whether problems are originating from the source of the video (indicating that there are content issues in the actual video payload), or due to issues on the transport network.

Using the MSAM, you can identify both source and transport network issues. Symptoms of source content errors include:

– Errors that occur on a single stream, rather than on all monitored streams. You can quickly identify errored streams, and filter your results to only show errored streams in the **All Streams Video** or **All Streams (Complete)** result groups.
– Transport Error Indicators. The transport error indicator is a bit that is set in the packet header by encoders if they detect corrupted content from the source. It always indicates that there is an issue with the video content.
– Continuity Counter Errors. These errors are usually detected by a monitoring system placed close to the video headend; therefore, they are typically corrected before reaching a downstream test instrument. When running analyzer applications, you can verify that there are no continuity counter errors by observing results in the **All Streams Video** or **All Programs** result groups.
– Continuous PCR (Program Clock Reference) jitter in the absence of excessive packet jitter. This is typically due to transcoding problems in the encoder. When running analyzer applications, you can observe PCR jitter measurements in the **All Streams Video** result group; packet jitter measurements are available in the **All Streams Transport** result group. If you are specifically comparing PCR jitter to overall packet jitter, select the **All Streams (Complete)** result group.
– PAT and PMT errors. Program specific information is comprised of tables of data associated with the programs carried in each stream; in particular, the PAT and PMT tables. This data must be present at regular intervals. PMT and PAT error counts are counts of sections that don't occur within the minimum required interval. You can observe these counts in the **All Streams Video** result group.

Symptoms of transport network problems include:

– Simultaneous packet loss and packet jitter. This is typically evaluated using the optional Media Delivery Index (MDI) analysis, which calculates the delay factor (DF) and media loss rate (MLR). The delay factor indicates how long a data stream must be buffered at its nominal rate to prevent packet loss. The media loss rate is a count of lost or out-of-sequence packets over time. Packet loss and jitter measurements are available in the **All Streams Transport** result group.
– Persistent packet loss and packet jitter. Packet loss and jitter measurements are available in the **All Streams Transport** result group.

MPEG-2 transport streams

When monitoring transport streams using the Dual Module Carrier, Transport Module, and MSAM, you can observe test results associated with transport stream header data and errors. Figure 64 illustrates a packetized transport stream. The module provides test results for each of the shaded header fields when running analyzer applications.

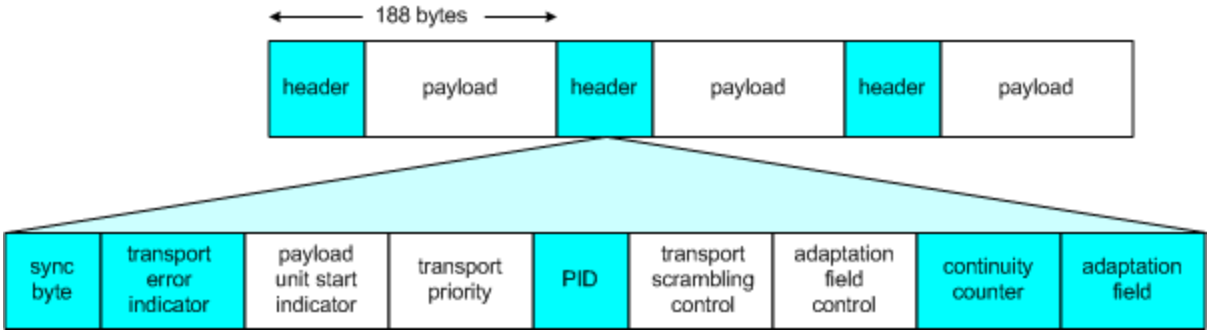


Figure 64 Packetized transport stream

Navigation Tip:

To observe results associated with MPEG-2 transport streams, run an analyzer application, and then select the top **Video Streams Quality** button on the Summary/Status display, or the **All Streams Video** result group.

The Transport Quality (IP, UDP, RTP) button and All Streams Transport result group provide test results associated with the *transport* of packets over the IP video network. They do not provide results associated with the actual *MPEG-2 transport streams*.

Packetized elementary streams (PES)

ES (elementary streams) carry video and audio payloads, which are then packetized, resulting in PES (packetized elementary streams). Each PES packet is then broken into fixed length transport packets, which are carried inside MPEG-2 transport streams.

Signaling tables

Three signaling tables are carried in a dedicated set of elementary streams for each transport stream. The tables, referred to as PSI (Program Specific Information), consist of a description of the elementary streams that are required to build particular programs, and descriptions of the programs.

Program Association Table (PAT)—Lists the program IDs of tables describing each individual program.

Program Map Table (PMT)—Lists the set of PIDs associated with a particular program.

When running an analyzer application, you can determine the PMT ID for a particular stream, and observe results associated with PAT and PMT errors.

IP Video encapsulation

MPEG-2 transport streams are typically encapsulated within RTP/UDP/IP or UDP/IP streams.

RTP

When MPEG-2 transport streams are encapsulated in RTP/UDP/IP/Ethernet streams, results are derived as follows:

– When running Explorer applications, packet jitter is measured using the average IP inter-arrival time; packet loss is measured using the RTP sequence number.
– When running Analyzer applications, packet jitter and packet loss are measured on the circuit using the RTP timestamps and sequence numbers, respectively.
– When running Analyzer applications, MDI DF results are measured using the average IP inter-arrival time; MDI MLR results are measured using the RTP sequence number. (MDI results are only available if you purchased the MDI option.)

When configuring a test, you can establish thresholds for declaring RTP loss distance and loss period errors. While running the test, you can easily determine whether transport streams are encapsulated in an RTP payload by observing the `RTP Present` result in the **All Streams Transport** result group.

Non-RTP

When MPEG-2 transport streams are encapsulated in UDP/IP/Ethernet streams, results are derived as follows:

– When running Explorer and Analyzer applications, packet jitter is measured using the average IP inter-arrival time; packet loss is measured using the MPEG continuity counter.
– When running Analyzer applications, MDI DF results are measured using the average IP inter-arrival time; MDI MLR results are measured using the the MPEG continuity counter.(MDI results are only available if you purchased the MDI option.)

Packet loss measurements are provided in the **All Streams Transport** result group; continuity counter errors are provided in the **All Streams Video** result group.

For descriptions of the IP Video test results, refer to Chapter 13 “Test Results”.

10

VoIP Testing

This chapter provides information on testing voice over IP services. Topics discussed in this chapter include the following:

– “About VoIP testing” on page 230
– “Understanding the graphical user interface” on page 231
– “Populating the Address Book” on page 235
– “Specifying interface settings” on page 236
– “Specifying Ethernet frame and IP settings” on page 236
– “Specifying VoIP settings” on page 237
– “Specifying VoIP Filters” on page 241
– “Placing and receiving calls” on page 241
– “Analyzing Audio Packets” on page 245

About VoIP testing

If your instrument is configured and optioned to do so, you can use it to verify the proper installation and configuration of Voice over IP (VoIP) service.

Features and capabilities

The VoIP option allows you to:

– Place and receive calls (call setup and teardown)
– Voice conversation/generate tone/IP voice announce
– Auto answer
– Real-time packet metrics (delay, jitter, packet loss)
– E-model QoS and RTCP statistics
– User selectable CODEC
– MOS and R Factor results

Understanding VoIP basics

VoIP refers to a collection of standards and technologies for transporting Voice over Internet Protocol. There are three basic functions that need to be performed in order for a voice conversation to take place:

Step1 The first requirement to maintaining a voice conversation is call management (signaling). This includes call setup, teardown and maintenance. These protocols/standards help enable the actual voice conversation. There are several standards for maintaining a phone call:

– H.323–This is an umbrella recommendation from ITU which contains a large set of standards for multimedia communication over packet switched networks.
– Session Initialization Protocol (SIP)–SIP is a contender to H.323 being developed by IETF multiparty, multimedia session control working group. This alternative is lighter and easier to setup than the H.323 standard.

Step2 VoIP is transmitted using several layers of encapsulation. A common example of how VoIP is transmitted is RTP > UDP > IP > L2 data-link protocol (IPoE/PPPoE).

Figure 65 is an example of the levels of encapsulation and where the voice sample is stored.

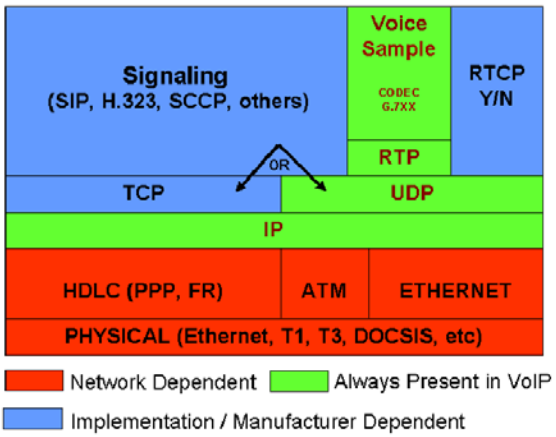


Figure 65 VoIP Encapsulation

Step3 Analog to digital data conversion/compression and vice versa. This involves sampling the audio and providing some digital outputs. This is done using codecs. Some examples of codecs used in VoIP are G.711 U law, G.711 A law, G.723 5.3K, G 723 6.3K, G.729A, G.726.32K, and G.722 64K.

Understanding the graphical user interface

When you configure your module for testing, the main screen provides four summary result buttons that allow you to display physical/link quality results, transaction log, transport streams quality results, and content streams quality results. Setup tabs are provided that allow you to specify items such as the destination phone number and codec. Other setups may appear, depending on the call control.

Action buttons

When running VoIP applications, buttons appear at the bottom of the Main screen that allow you to select an SFP or specify the wavelength for an optical connector (if applicable), turn the laser on or off, and, register with the management entity (also called “gateway,” “proxy,” or “call manager,” depending on which signaling protocol you are using), or place and receive a call.

Understanding the LED panel

When you select a VoIP application, LEDs appear next to the result window on the Main screen (see Figure 66).

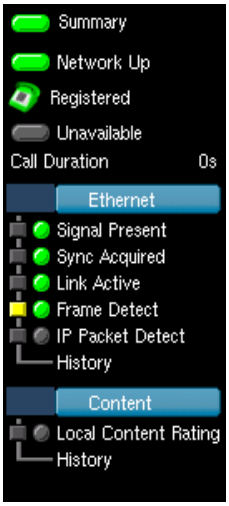


Figure 66 VoIP LEDs

The LEDs allow you to quickly determine whether a signal is present, whether synchronization has been acquired, and whether or not the link is active. LEDs also indicate the content rating.

Understanding the VoIP call bar

The VoIP call bar is located in the area just above the results. It allows entry of the destination phone number and quick selection of setup items. The setup items available vary depending on the call control.

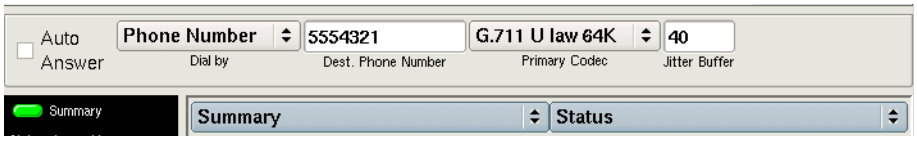


Figure 67 VoIP call bar, SIP call control

Understanding VoIP test results

VoIP results are available that allow you to verify the quality of the physical layer, the link, the transport quality of audio streams, and the quality of the audio itself.

Layered view: Quality Layer Buttons

The layered view appears on the Main screen the first time you launch a VoIP application. Color coded quality buttons appear which immediately indicate the current and historical status of the physical layer and link, the transport of the audio streams (using IP, UDP, and RTP), and the audio streams themselves. Figure 68 illustrates the view when all results are OK and there is no history

of errors at any layer.

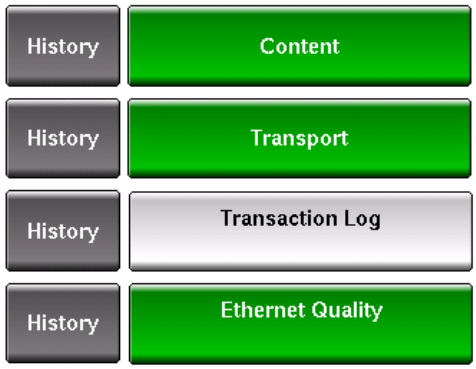


Figure 68 Layered View - All Results OK

Ethernet Quality (Physical Link Quality) —Selecting this button will display aggregate results (such as the bandwidth utilization, interface (layer 1) and Ethernet (layer 2) errors for the link.

Transaction Log—Selecting this button will display a running list of all transactions with the far-end including communication with Call Manager/Gatekeeper/Proxy, and call status.

Transport Quality—Selecting this button will display test results for each monitored IP, UDP, or RTP voice stream.

Content Quality—Selecting this button will display test results for each monitored voice stream.

Navigation Tip:

You can always return to the layered view by setting the results group to **Summary**, and the category to **Status**.

Layered View: Button Colors

Figure 69 illustrates the view when the instrument has lost the physical connection so there is a history of errors at the physical layer.

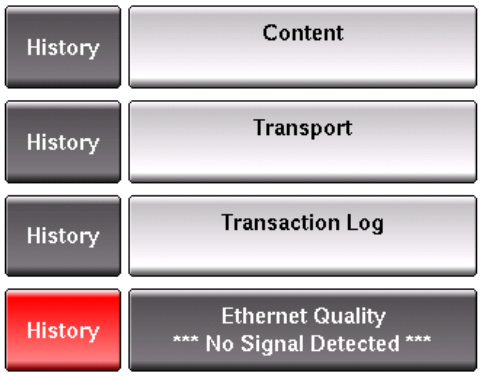


Figure 69 Layered View - Errored physical link

Table 24 explains each of the colors used for the current and history buttons.

Table 24 Current and History Button Colors

Color	Current	History
Green	Indicates that all results are OK for that particular quality group. For an example, see Figure 68 on page 233.	N/A
Yellow	Indicates that at least one result at that particular layer triggered a minor alarm or error based on the established thresholds.	Indicates that at least one result occurred during the test that triggered a minor alarm or error based on the established thresholds.
Red	Indicates that at least one result at that particular layer triggered a major alarm or error based on the established thresholds.	Indicates that at least one result triggered a major alarm or error based on the established thresholds during the test. For an example, see Figure 69 on page 233.

To optimize the number of results that appear on your display, the result windows appear in the Full Size view by default when you run VoIP applications.

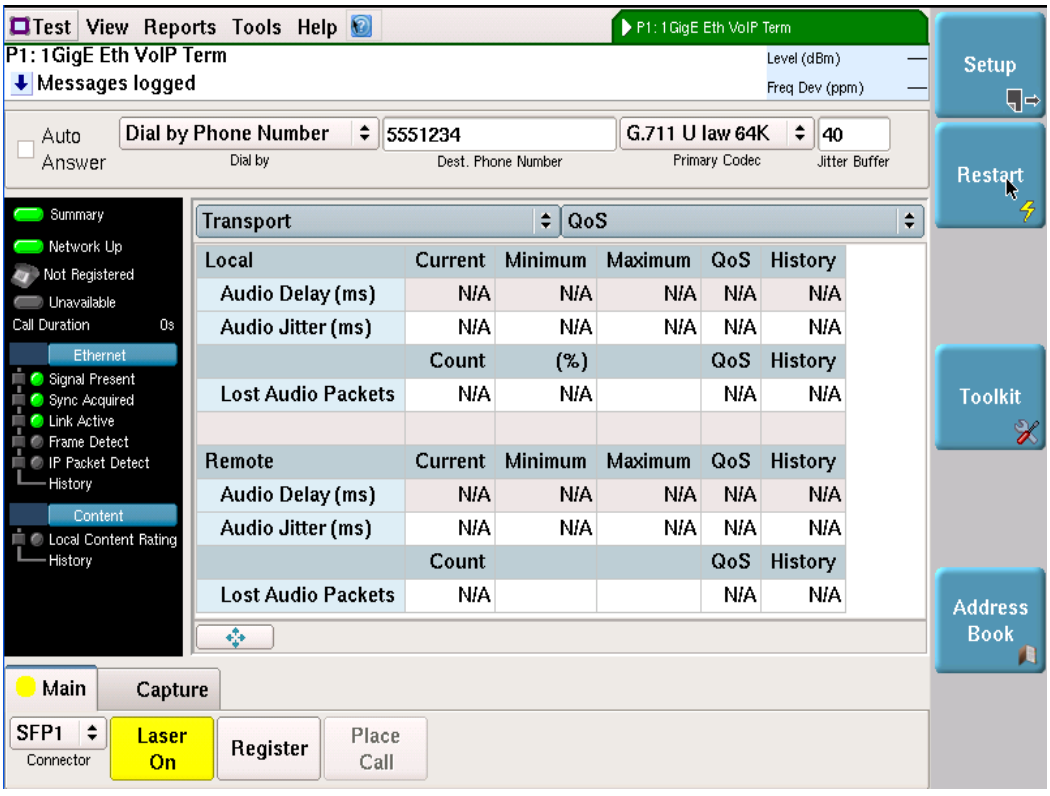


Figure 70 VoIP results: Transport quality

Navigating the results display

When navigating through the VoIP results, consider the following:

– When you launch an application for the first time, the Summary group and Status category appear. This is also referred to as the “layered” view (see “Layered view: Quality Layer Buttons” on page 232).
– When you launch applications subsequent times, the result view that was displayed the last time you ended a test appears. For example, if the Transport quality results were displayed the last time you ran the application, the next time you launch the application, the Transport quality results will appear (see Figure 70 on page 234).
– Use the result group button to switch between the Summary, Content, Transport, Transaction Log, Miscellaneous, Ethernet, and Graphs groups.
– Use the result category button to switch between the categories for each group. For example, when observing results in the Content group, Current Call Scores and Historical Call Score Stats categories are available.

VoIP test applications

If your instrument is optioned to do so, this release supports the VoIP applications listed in Table 25.

Table 25 VoIP applications

Interface	Application	Test Mode
10/100/1000	VoIP	Terminate
100M Optical	VoIP	Terminate
1GigE Optical	VoIP	Terminate
10G LAN	VoIP	Terminate

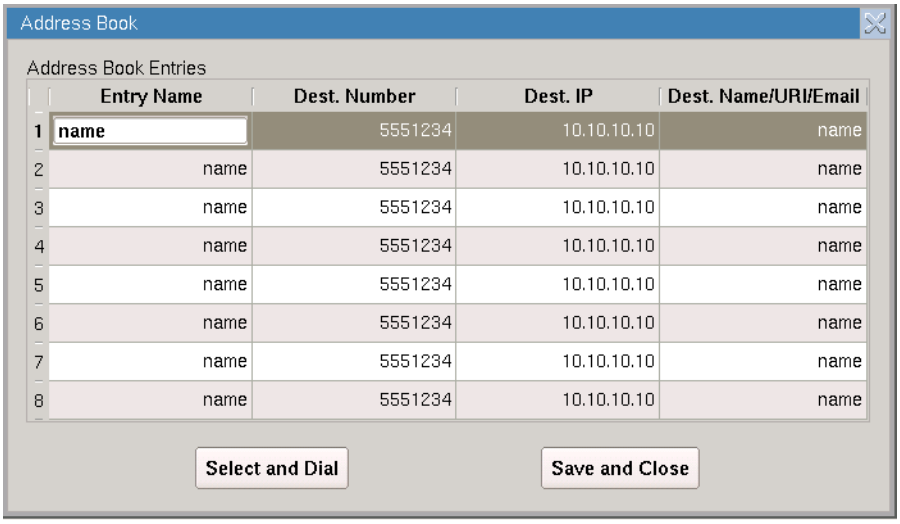
Populating the Address Book

The Dual Module Carrier, Transport Module, and MSAM provides an Address Book which gives you quick access to phone numbers when you want to place a call. Entries can include name, phone number, and IP address information. The address book can be saved by saving the test configuration.

To update entries in the address book

Step1 If you haven’t already done so, launch a VoIP application. For a list of applications, see Table 25 on page 235.

Step2 Press the **Address Book** soft key. The address book appears.



Step3 In the Entry Name column, tap the field to launch a keypad, and then specify a name for the entry.

Step4 In the Dest. Number column, tap the field to launch a keypad, and then enter a phone number alias for the entry.

Step5 In the Dest. Name/URI/Email column, tap the field to launch a keypad, and then enter the destination name/URI/Email.

Step6 Select either **Select and Dial** or **Save and Close**.

The entry is updated.

Specifying interface settings

Before testing on an optical circuit, you can specify interface settings which:

– Indicate which SFP jack you are using (if your unit is equipped with SFP jacks).
– Specify the transmitted wavelength (if your unit is equipped with 850 nm, 1310 nm, and 1550 nm connectors).
– Allow your unit to communicate with another Ethernet device (when requesting video traffic using IGMP).

For details on the various connectors used to connect to the circuit, refer to the printed Getting Started User's Manual that shipped with your unit. For details on specifying the information required to establish a link to another device, see "Specifying interface settings" on page 46 of Chapter 4 "Ethernet and IP Testing".

Specifying Ethernet frame and IP settings

Before you transmit traffic, you can specify the frame characteristics of the traffic, such as the frame type (DIX, 802.3), encapsulation (VLAN, Q-in-Q,), and IP settings such as IP type, gateway, and subnet mask.

To specify Ethernet frame settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 25 on page 235 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **Ethernet/IP** tab.

Step3 In **Encapsulation**, select one of the following:

- **None**. If you do not want to encapsulate transmitted frames, select **None**.
- **VLAN.** If you want to transmit VLAN tagged frames, select VLAN, and then refer to "Configuring VLAN tagged traffic" on page 54.
- **Q-in-Q.** If you want to transmit VLAN stacked (Q-in-Q) frames, select **Q-in-Q**, and then refer to "Configuring Q-in-Q traffic" on page 55.

Step4 In **Frame Type**, specify the type of frame you are transmitting (DIX, or 802.3).

Step5 In **Source Type**, specify whether the source MAC address uses a factory default MAC or User Defined. If User Defined, enter the MAC address

Step6 If you selected VLAN Encapsulation, enter the **VLAN ID** and **Priority**.

Step7 If you selected Q-in-Q Encapsulation, do the following:

a Enter the **SVLAN** ID, DEI, Priority, and TPID.

b Enter the **CVLAN** ID and Priority.

Step8 Specify whether the **Source IP Type** is a Static address or DHCP.

Step9 If you selected **Static** IP, specify the Source IP, Gateway, and Subnet Mask.

The Ethernet frame and IP settings are specified.

Specifying VoIP settings

Before placing or receiving VoIP calls, you must specify the VoIP settings.

To specify VoIP settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 25 on page 235 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **VoIP** tab.

Step3 In the panel on the left side of the tab, select **General**, and then specify the following:

a Select **Auto Answer**, and then specify whether to automatically answer calls.

b Select **Call Control Standard**, and then specify a call control standard

- **SIP** is Session Initiation Protocol. It is an application layer protocol used to establish, modify, and terminate conference and telephony sessions over IP-based networks.
- **SCCP** is the call control used on Cisco VoIP systems.
- **H.323 (Fast connect)** minimizes the number of messages exchanged.

c If you selected SIP call control, specify the following settings.

Setting	Description
Source Alias	Enter the source phone number alias.

Setting	Description
Outbound Alias	Select how to dial the destination: Dial by Phone Number or Dial by Name/URI/Email.
Dest. Phone Number	If you selected “Dial by Phone Number” for Outbound Alias, enter the destination phone number via the on-screen keypad or select from the list of recently dialed numbers.
Dest. Name/URI/Email	If you selected “Dial by Name/URI/Email” for Outbound Alias, enter the destination name/URI/Email via the on-screen keypad or select from the list of recently entered names.
SIP Vendor	Specify the vendor.
100 Rel Usage	Specify whether 100rel is required, supported, or disabled. 100 Rel provides reliable provisional response messages by appending the 100rel tag to the value of the required header of initial signalling messages.

d If you selected SCCP call control, specify the following:

Setting	Description
Dest. Phone Number	Enter the destination phone number via the on-screen keypad or select from the list of recently dialed numbers.
Device Type	Specify the Device Type.
Device Name	If checked, click on the field and use the keypad to enter the device name.

e If you selected H.323 call control, specify the following settings..

Setting	Description
Source Alias	Enter the source phone number alias.
Dest. Phone Number	Enter the destination phone number via the on-screen keypad or select from the list of recently dialed numbers.
H.323ID	Enter the ID, using up to 40 characters. This is an ID element field that is sent to the Gatekeeper during all registration and request messages.
Bear Cap	Specify the bearer capability: Voice, 3.1K audio, Unrestricted Digital This sets the Bearer Cap information element in the H.323 setup message for outgoing calls.
Calling Party Number Plan	Specify the numbering plan, if required: Unknown, ISDN/Telephony, Data, Telex, National, Private This sets the Calling Party Numbering Plan information element in the H.323 setup message for outgoing calls.
Calling Party Number Type	Specify the type of number, if required: Unknown, International, National, Network Specific, Subscriber, Abbreviated. This sets the Calling Party Type information element in the H.323 setup message for outgoing calls

Setting	Description
Called Party Number Plan	Specify the numbering plan, if required: Unknown, ISDN/Telephony, Data, Telex, National, Private. This sets the Called Party Numbering Plan information element in the H.323 setup message for outgoing calls.
Called Party Type	Specify the type of number, if required: Unknown, International, National, Network Specific, Subscriber, Abbreviated. This sets the Called Party Type information element in the H.323 setup message for outgoing calls.

Step4 If you selected SIP call control, in the panel on the left side of the tab, select **Proxy**, and then specify the following:

Setting	Description
Proxy Mode	Specify whether your circuit has a Static Proxy or No Proxy.
Address Type	If your circuit uses a static Proxy, specify whether the address is an IP Address or DNS Name.
Proxy IP	Enter the IP address of the proxy. To verify the proxy address, press the **PING** soft-key. If the address is reachable, a check mark will display next to the Ping button. If not, a red X will display. This is the outbound proxy, or the device from which the instrument will send and receive all SIP messages. If you have a network that uses one server for registration and another for placing and receiving calls, the Proxy IP specifies the address for placing and receiving calls.
Proxy User name	Enter a user name used to access the Proxy.
Proxy Password	Enter the password associated with the user name.
DNS Name	If the address type is DNS Name, enter the DNS name for the proxy.
Proxy Port	Enter the proxy port number.
Call Control Port	Enter the call control port number.

Step5 If you selected SCCP call control, in the panel on the left side of the tab, select **Call Manager**, and then specify the following:

Setting	Description
Call Manager IP	Enter the IP address of the call manager.
Call Manager Port	Enter a number for the call manager port.

Step6 If you selected H.323 call control, in the panel on the left side of the tab, select **Gatekeeper**, and then specify the following:

Setting	Description
Gatekeeper Mode	Specify the gatekeeper mode: **NO GATEKEEPER** means no RAS (registration, admission, and status) messages will be used. **AUTO DISCOVER** automatically discovers the gatekeeper. **STATIC** allows you to enter the gatekeeper address.

Setting	Description
Authentication	Specify whether authentications is supported or required.
Gatekeeper IP	Enter the gatekeeper IP address
Username	Enter the username to register with the gateway.
Password	Enter the password associated with the username.
Local RAS Port	Enter the UDP port that is used locally for registration (RAS messages)
Call Control Port	Enter the UDP port that is used for call control messages (for placing and receiving calls).
Gatekeeper RAS Port	Enter the UDP port that the gatekeeper uses for registration (RAS messages).
Time Zone	Select the time zone where you are located.

Step7 In the left panel on the side of the tab, select **Audio Codec** and then specify the following:

Setting	Description
Primary Codec	Select the codec type to be advertised/supported for receiving audio packets. The codec on the receiving and transmitting end should match. The call may not be successful if the codecs don't match
Speech Per Frame	Specify the number of milliseconds of speech per transmission frame the unit can receive.
Jitter buffer	Set the jitter buffer length.This is the number of milliseconds of speech that will be collected before an attempt will be made to play the speech back. This allows lost, late, or out-of-sequence packets time to arrive and be reassembled before playback.
Transmit Source	Select the transmit source: Voice conversation (transmits and receives live voice), IP voice announce (the unit repeats a sequence of words including the calling party's IP address), Tone (transmits the specified frequency).
Language	If the Transmit Source is set to IP Voice Announce, the Language selection becomes available. This specifies the language for the transmitted voice announcement.
Voice IP QOS	Enter a value to indicate the Voice IP Quality of Service. The value you enter will be both the Differentiated Services (DiffServ) code point and the type of service (ToS) indicator. The value will occupy a 6-bit field in the packet headers of RTP stream voice packets and will indicate how packets are treated at each hop. You can specify a number from 0 to 63 to indicate the per-hop behavior.
RTP Port Min/Max	Specify the RTP port minimum and maximum numbers. The real-time transport protocol (RTP) port number allows you to identify voice traffic versus other traffic. Some systems only accept RTP traffic on certain port numbers.
Silence Suppression	Specify whether silence suppression is supported.

Step8 In the left panel on the side of the tab, select **QoS** and then specify the following:

Setting	Description
MOS Scaling	Specify the scale used for MOS results.
Jitter Threshold	Specify the pass and fail thresholds for the jitter result.
Delay Threshold	Specify the pass and fail thresholds for the delay result.
Loss Threshold	Specify the pass and fail thresholds for the loss result.
Content Threshold	Specify the pass and fail thresholds for the MOS results.

The VoIP settings are specified.

Specifying VoIP Filters

If you wish to capture VoIP packets, you can specify filters to capture specific types of packets.

To specify VoIP filter settings

Step1 If you haven't already done so, use the Test Menu to select the test application for the interface you are testing. Refer to Table 25 on page 235 for a list of applications.

Step2 Select the **Setup** soft key, and then select the **VoIP Filters** tab.

Step3 Specify the type of filter:

Setting	Description
Signaling	Only incoming and outgoing signaling/control packets shall be captured. Incoming signaling/control packets destined for the unit (based on destination IP address of incoming packets) shall only be sent to the capture buffer. Signaling packets shall include RTCP packets, H.323/SIP/SCCP call control packets.
Audio	Only audio packets for the call in progress shall be sent to the capture buffer. Incoming packets shall be captured based on destination IP address and UDP port number fields of the packets.
Signaling and Audio	Both signaling and audio packets shall be sent to the capture buffer.
All Traffic	All incoming traffic will be captured.

The VoIP filters are specified.

Placing and receiving calls

To verify call setup and tear down, the instrument allows placing and receiving calls. To monitor the audio and insert voice into calls, the unit allows use of wired and Bluetooth wireless headsets.Adjustment of the audio volume levels is accomplished via on-screen controls.



NOTE:

If playing audio on a MTS8000 with DMC, no audio path is available. You can use the simulated voice and observe results but will not hear audio.

Registering with the server

Before placing or receiving calls, you must register with the server (the Proxy/Gateway/Call Manager, depending on call control). If H.323 call control is used, you must manually register with the server after changing any call settings. If SIP or SCCP call controls are used, the unit automatically deregisters and registers with the server after a change in call settings.

To register with the server

– Tap the **Register** action button to begin registering.



Figure 71 VoIP registration action button

NOTE:
The registration action button is not available if using H.323 call control with NO Gatekeeper.

After successful registration, the button will turn yellow and change to “Registered” and the Stack status indicator in the LED panel updates.

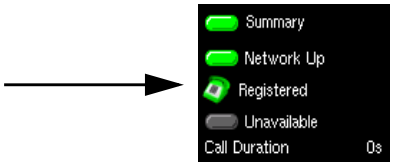


Figure 72 Successful registration

NOTE:
When Proxy Mode is set to “No Proxy”, registered LED will not be lit.

Placing calls

After specifying configuration settings and registering with the server, you can place a VoIP call.

To place a VoIP call

Step1 Select the **Place Call** action button.

The button label changes to Hang Up.

After the call is connected, the Call status in the LED panel will update and the timer begins counting.

Step2 While the call is up, observe the Transport and Content result categories.

If voice insertion is configured, the Audio levels and Bluetooth connection settings can be adjusted by selecting the speaker and Bluetooth icons in the system tray.

Step3 If desired, DTMF tones may be sent using the DTMF keypad.

NOTE
For DTMF tone entry, the configuration must specify call type = Voice Conversation.

Step4 Select the **Hang up** action button to end the call.

Receiving calls manually

After specifying configuration settings and registering with the server, you can receive a VoIP call.

To receive a VoIP call

Step1 When the instrument indicates an incoming call, select the **Answer Call** action button.

The button label changes to Hang Up.

After the call is connected, the Call status in the LED panel will update and the timer begins counting.

Step2 While the call is up, observe the Transport and Content result categories.

If audio monitoring or voice insertion is configured. the Audio levels and Bluetooth connection settings can be adjusted by selecting the speaker and Bluetooth icons in the system tray.

Step3 Select the **Hang up** action button to end the call.

Automatically answering calls

The Auto Answer feature allows you to verify incoming service.

To answer calls automatically

Step1 In the VoIP call bar, check the box for **Auto Answer**.

Step2 Place a call to the instrument from a VoIP phone (or a second instrument).

The call is automatically answered, and the following information is logged:

- Time the call was answered
- Caller's IP address
- Time the call ended

Step3 Tap the **Hang up** action button to end the call.

Capturing packets for analysis

If your instrument is configured and optioned to do so, you can use it to capture transmitted and received packets, save it on the instrument or to an external USB key, and then either send the packets to another technician for analysis, or analyze it yourself using the PVA-1000 VoIP Analyzer software.

Understanding the Capture toolbar

The buttons on the Capture toolbar (illustrated in Figure 73) are used to enable or disable the capture feature, start and stop the capture process, save the packets in the capture buffer to the internal USB drive (or an external drive), or launch Wireshark® or J-Mentor to analyze the packets on the instrument.



Figure 73 Capture Toolbar

The % Buffer Full gauge shows the percentage of the available buffer capacity that is used.

When you capture traffic at a high bandwidth or specify a small buffer size, if you configure the capture to wrap (overwrite) the oldest packets in the buffer with new captured packets in 1 MB increments, the buffer gauge may appear to "jump around". If you do not wrap the packets, the capture process may stop very soon after you start it, because the buffer reaches capacity quickly. This is expected behavior.

Specifying filter settings

If you specify VoIP filter settings (see "Specifying VoIP Filters" on page 241), the settings determine which *received traffic* is captured to the buffer. The Capture Toolbar (illustrated in Figure 73) indicates whether filters are active or inactive. Transmitted frames are always captured to the buffer.

Capturing packets

Capturing packets involves launching and configuring a VoIP application, specifying the capture settings, and, if you are capturing received traffic, specifying the filter settings.

While capturing packets in the VoIP application, it is recommended that you do not save the captured packets until the call is ended (the phone is on hook).

When capturing packets, bear in mind that configuring the capture for a large buffer (for example, 256 MB) with small packets (for example, 46 byte ping packets), it will take a long time to fill the buffer. If you configure the capture for a small buffer with large packets, it will take much less time.

To capture packets on the instrument

Step1 Select the **Setup** soft key, and then do one of the following:

- Specify the settings required to filter received traffic for the type you want to capture and analyze.
- Clear all of the filters to capture all received traffic.

For details, refer to "Specifying filter settings" on page 244.

Step2 Select the **Capture** setup tab, and then specify the following settings:

Setting	Parameter
Capture buffer size (MB)	Specify a size ranging from 1 to 256 MB in a 1 MB increment. The default buffer size is 16 MB.
Capture frame slicing	If you want to capture the first 64 or 128 bytes of each frame (and ignore the rest of the frame), select 64 or 128; otherwise, select None. If you select None (the default), the entire frame is captured.
When capture buffer is filled	If you want to overwrite the oldest packets with new packets when the buffer becomes full, select **Wrap Capture**; otherwise, select **Stop Capture**.

Step3 Select the **Results** soft key to return to the Main screen.

Step4 Select the Capture toolbar, and then select **Start Capture**.

A message appears in the message bar indicating that the capture has started, and the action key states **Capture Started**.

Step5 If you want to manually stop capturing packets (for example, after the instrument has transmitted and received a certain number of frames), select the **Capture Started** action key.

The action key turns gray, and a message appears in the message bar indicating that the capture is complete.

Packets were captured and are stored temporarily in the capture buffer. A count of the number of packets processed is provided in the Ethernet result group, in the Capture category.



WARNING: Changing applications or turning OFF the instrument

You will lose the entire contents of the capture buffer if you launch a new application on the port that you are capturing packets on, or if you turn your instrument OFF. To ensure that the packets are stored, save the capture buffer before changing applications or turning the instrument OFF.

Step6 Select **Save Capture Buffer** and then specify the file name and other parameters as needed.(For more information, see “Saving or exporting captured packets” on page 100.)

Analyzing Audio Packets

Audio packets captured with the VoIP application can be analyzed using the PVA-1000 VoIP Analyzer software from JDSU. PVA-1000 software provides automated capture and detailed analysis of VoIP calls. It provides details of signaling and quality performance issues.

When capturing packets in the VoIP application, it is recommended that you do not save the captured packets until the call is ended (the phone is on hook).

11

Fibre Channel Testing

This chapter provides information on testing Fibre Channel services. Topics discussed in this chapter include the following:

– “About Fibre Channel Testing” on page 248
– “Features and capabilities” on page 248
– “Configuring layer 1 tests” on page 250
– “Configuring layer 2 Fibre Channel tests” on page 252
– “Transmitting and analyzing layer 2 traffic” on page 256
– “Loopback testing” on page 257
– “Transmitting and analyzing patterns” on page 257
– “Measuring service disruption time” on page 258
– “Inserting errors” on page 259
– “Measuring round trip delay” on page 259
– “Monitoring layer 2 traffic” on page 260
– “Emission Lowering Protocol” on page 260

About Fibre Channel Testing

If your instrument is configured and optioned to do so, you can use it to provision Fibre Channel service, verify end-to-end connectivity, and analyze link performance by simulating different traffic conditions. Figure 74 illustrates the Main screen when running a 10 Gigabit Fibre Channel application.

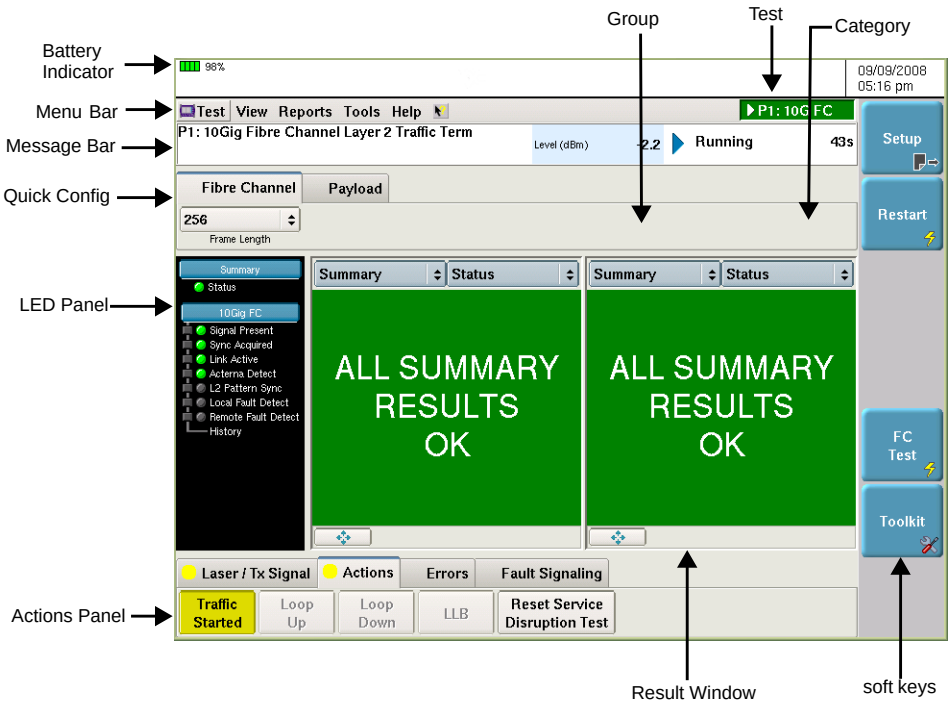


Figure 74 Main screen, 10 Gigabit Fibre Channel application

This release of the instrument supports 1, 2, 4, 8 and 10 Gigabit Fibre Channel testing.

Features and capabilities

Features and capabilities of the Dual Module Carrier, Transport Module, and MSAM include the following when testing Fibre Channel service:

- 1 Gigabit, 2 Gigabit, and 4 Gigabit testing—You can run Layer 1 BER, Layer 2 Traffic, and Layer 2 Pattern tests over 1, 2, and 4 Gigabit Fibre Channel circuits. Dual port testing is possible in Terminate and Monitor/Thru modes.
- 8 Gigabit testing—You can run Layer 2 Traffic tests in Terminate and Monitor/Thru modes and Layer 2 Pattern tests in Terminate mode over 8 Gigabit Fibre Channel circuits using an XFP in an MSAM v2 assembly.
- 10 Gigabit testing—You can run Layer 1 BER and Layer 2 Traffic tests over 10 Gigabit Fibre Channel circuits in Terminate and Monitor/Thru modes using either port of an XFP in an MSAM v2 assembly.
- Fibre Channel login and flow control—The instrument supports Exchange of Link Parameters (ELP) through distance extension equipment when turning up a circuit, allowing you to login to another module at the far end. Before logging into another module, you can specify the number of buffer credits to verify that flow control is functioning properly.

– Frame verification—You can verify that the size and format of Fibre Channel frames conform to ANSI X3T11 requirements, ensuring that network elements can support reliable communications.
– BER testing—You can verify circuit performance by sending BERT patterns over switched (layer 2) and unswitched (layer 1) networks.
– Scrambling— You can select to scramble all words transmitted between Start of Frame (SOF) and the End of Frame (EOF) delimiters in Terminate applications and descramble received traffic in Monitor/Through applications.
– Emissions Lowering Protocol (ELP)— You can configure ELP by specifying the ordered set to be transmitted during the Link INIT and for fill words. The three configurable modes are OFF (IDLE/IDLE), ON/Enabled IDLE/ARBff and ON Enabled ARBff/ARBff.
– Explicit Fabric/N-Port login; fabric topology—You can use your instrument to login to an N_Port, and then verify that it can establish an operating environment with a fabric and communicate with other destination N Ports by indicating that the service you are testing uses a fabric topology. When testing on a fabric topology, you specify source *and* destination N Port and Node names for the login process.
– Explicit Fabric/N-Port login; point-to-point topology—You can use your instrument to login to an N_Port, and then verify that it can communicate with other destination N Ports by indicating that the network you are testing uses a point-to-point topology. When testing on a point-to-point topology, you specify a source N Port and Node name, and a destination and source ID for the login process.

Understanding the graphical user interface

When you configure your instrument for testing, graphical displays of Fibre Channel frames are provided on the setup tabs for the application you selected. You can specify frame characteristics for transmitted and filtered traffic by selecting the corresponding field on the graphic, and then entering the value for transmitted or filtered traffic. Colored and white fields can be edited; fields in gray can not be modified.

Figure 75 illustrates the Frame Details for a layer 2 traffic test.

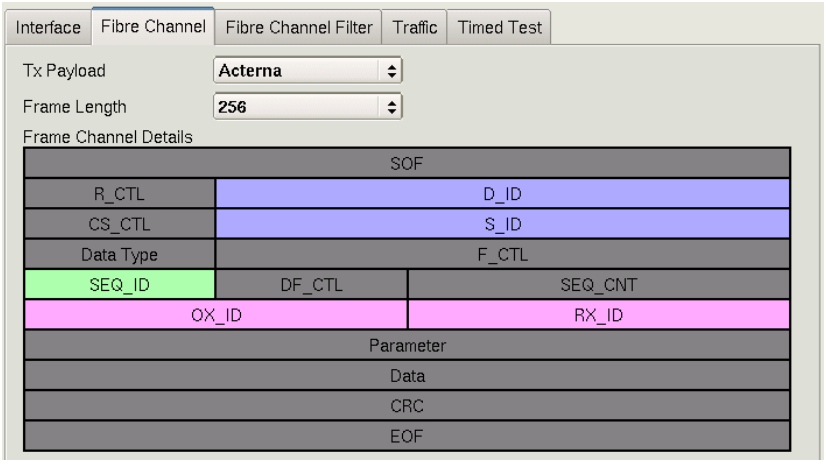


Figure 75 Frame Details

For details on specifying frame characteristics, see “Specifying Fibre Channel frame settings” on page 254 and “Specifying Fibre Channel filter settings” on page 255.

Fibre Channel test applications

This release supports the applications listed in Table 26 when testing 1 Gigabit, 2 Gigabit, 4 Gigabit, 8 Gigabit and 10 Gigabit Fibre Channel circuits.

Table 26 Fibre Channel applications

Signal/Rate	Application	Test Mode[a]
1Gig, 2Gig, and 4Gig	Layer 1 BERT	Terminate Monitor/Through
	Layer 2 Patterns	Terminate
	Layer 2 Traffic	Terminate Monitor/Through
8Gig	Layer 2 Patterns	Terminate
	Layer 2 Traffic	Terminate Monitor/Through
10Gig	Layer 1 BERT	Terminate Monitor/Through
	Layer 2 Traffic	Terminate Monitor/Through

a. You must use two Fibre Channel SFPs or XFP s (8Gig and 10Gig) to test in monitor/through.

Configuring layer 1 tests

When testing Fibre Channel service, you can generate and receive layer 1 test patterns utilizing 1, 2, 4 and 10 Gigabit Fibre Channel-capable PIMs. You can also monitor and analyze Layer 2 Traffic and Patterns utilizing 1, 2, 4, 8 and 10 Gigabit Fibre Channel-capable PIMs.

When running a Layer 1 BERT test on a Fibre Channel circuit, you must actively start transmission of the test pattern by pressing the **Start BERT Pattern** action button.



NOTE:

Refer to IEEE 802.3ae-2002, Sections 49.2.8, 49.2.12, and 52.9.1 for detailed descriptions of each pattern available when testing 10 Gigabit Fibre Channel circuits. For 1 Gigabit, 2 Gigabit, and 4 Gigabit MF, LF, and HF Fibre Channel patterns, refer to the IEEE 802.3, 2000 Edition, Annex 26A. For 1 Gigabit RDPAT, JTPAT, and SNPAT patterns, refer to the NCITS TR-25-1999 specifications.

BER testing layer 1

Use the layer 1 BERT terminate application to generate and receive layer 1 test patterns.

To BER test layer 1

Step1 Using the Test Menu, select the layer 1 BERT terminate test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 To specify the BER pattern, select the **Setup** soft key, select the Interface tab, and do the following:

a If you want the unit to use the Tx BERT pattern as the Rx BERT pattern, in BERT Rx<=Tx, select **On**; otherwise, select **Off**.

b Select a Tx Pattern.

c If the Rx=Tx setting is Off, select an Rx Pattern.

d If you are using SFPs and are testing in Monitor/Through mode, select the tab corresponding to the second SFP jack, and then repeat step a through step c.

Step3 Connect the module to the circuit.

Step4 On the Main screen, select the **Laser** button.

Step5 Verify that the green Signal Present and Pattern Sync LEDs are illuminated.

Step6 At a minimum, observe the test results in the following categories:

- Summary
- Error Stats

Layer 1 BER testing is complete.

When running the L1 BERT application, your LEDs may indicate that you have **L1 Pattern Sync** without word sync. The word sync status is indicated on your unit using a red **Sync Acquired** LED (if word sync was obtained, then lost), or an extinguished LED (if word sync was never obtained since starting your test). This is usually due to a temporary loss of signal or word sync when receiving an L1 pattern that does not contain Fibre Channel compliant link characters (for example, IDLE). To resolve this, stop transmitting the L1 pattern momentarily to allow the receiver to regain sync, and then begin transmitting the pattern again.

If this occurs, be certain to determine why the signal or word sync was lost temporarily.

Monitoring layer 1 BER

Use the layer 1 BERT monitor application to analyze the received signal.



NOTE:

To pass the signal through to the unit's transmitter, you must turn the laser on using the button on the Main screen.

To monitor layer 1 BERT

Step1 Using the Test Menu, select the layer 1 BERT monitor/through test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 To specify the BER pattern for the traffic you are monitoring, select the **Setup** soft key, select the Pattern tab, and then select the Rx Pattern.

Step3 Connect the module to the circuit.

Step4 On the Main screen, select the **Laser** button.

Step5 Verify that the green Signal LED is illuminated.

Step6 At a minimum, observe the test results in the following categories:

- Summary
- Error Stats

You are monitoring layer 1 traffic carrying the BERT pattern that you specified.

Configuring layer 2 Fibre Channel tests

Using the instrument, you can transmit, monitor, and analyze layer 2 Fibre Channel traffic. Step-by-step instructions are provided in this section for the following:

– "Specifying interface settings" on page 252
– "Specifying Fibre Channel frame settings" on page 254
– "Specifying Fibre Channel filter settings" on page 255
– "Specifying traffic load settings" on page 256

Specifying interface settings

Before you transmit layer 2 traffic, you can specify interface settings which:

– Turn flow control on, and specify the login method (Implicit, Explicit E-Port, or Explicit Fabric/N-Port) and the number of transmit or receive buffer to buffer credits to communicate to the module's link partner during the login process. When you turn flow control on, the module:
  – Generates an R_RDY message for each frame received.
  – Provides a count of received R_RDY messages.
– Specify the connector to use for the test (if more than one transceiver is inserted in the PIMs).
– Specify a unit identifier to identify all traffic originating from the module. It uses its default source ID when doing E-Port login and its user-specified port name when logging into a fabric.

To specify interface settings

Step1 If you haven't already done so, use the Test Menu to select the layer 2 terminate test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 Select the **Setup** soft key, then select the Connector sub-tab to specify which optical connector you are using for the transceiver.

Step3 Select the **Physical Layer** sub-tab, and then specify the settings required for the type of login and, if applicable, topology that you specify:

Table 27 Fibre Channel Physical Layer settings

Setting	Values	Implicit	Explicit (E-Port)	Explicit (Fabric/N-Port)	
				Point-to-Point Topology	Fabric Topology
FlowControl	– Select **On** if you want the instrument to operate as a credit-based transmitter. – Select **Off** to generate frames without crediting. **NOTE:** You must turn flow control ON to specify Login settings.	√	√	√	√

Table 27 Fibre Channel Physical Layer settings (Continued)

Setting	Values	Implicit	Explicit (E-Port)	Explicit (Fabric/N-Port)	
				Point-to-Point Topology	Fabric Topology
Login (FlowControl is On)	– To verify that both devices use flow control and no login is required, select **Implicit**, and then specify the Tx Buffer to Buffer credits. – To discover another instrument or device's settings, select **Explicit (E-Port)**, and then specify the Rx Buffer to Buffer credits. – To login to an N-Port on a circuit using a Point-to-Point or Fabric topology, select **Explicit (Fabric/N-Port)**, and then specify the Rx Buffer to Buffer Credits.	√	√	√	√
Tx Buffer to Buffer Credits (Near-end B-B)	If you specified an **Implicit** login, select this field, and then type the number of buffer credits the far end device can support. This number should match the receive buffer size for the far end device.	√	N/A	N/A	N/A
Rx Buffer to Buffer Credits (Far-end B-B)	If you specified an **Explicit (E-Port)** or **Explicit (Fabric/N-Port)** login, select this field, and then type the number of buffer credits the instrument will advertise that it can support during the ELP login exchange with the far end device.	N/A	√	√	√
Topology	– To login to an N Port, and then verify that it can communicate with other destination N Ports, select **Point-to-Point**. – To login to an N_Port, and then verify that it can establish an operating environment with a fabric and communicate with other destination N Ports, select **Fabric**.	N/A	N/A	√	√
Source N Port Name	Specify the source port name carried in the login request.	N/A	N/A	√	√
Source Node Name	Specify the source node name carried in the login request.	N/A	N/A	√	√
Destination N Port Name	Specify the destination port name carried in the login request.	N/A	N/A	N/A	√
Destination Node Name	Specify the destination node name carried in the login request.	N/A	N/A	N/A	√
Destination ID	Specify the destination ID carried in the login request.	N/A	N/A	√	N/A
Source ID	Specify the source ID carried in the login request.	N/A	N/A	√	N/A

NOTE:

When you test flow control on a Fibre Channel circuit, specify the *same number of buffer credits* for both the near-end and far-end instruments. If you specify a different number of credits, or if you specify a very low number, you may not achieve desired bandwidth utilization.

Step4 *Optional*. If you want to transmit an ID for all loop up and loop down frames originating from the module, select the Unit Identifier field, and then type the ID. The default ID is JDSU 6000.

Step5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The interface settings are specified. You can verify the login status and observe test results associated with the login process by displaying the Fibre Channel Login Status result category (see "Login Status results" on page 388).

Specifying Fibre Channel frame settings

Before you transmit layer 2 traffic, you can specify the frame characteristics of the traffic, such as the frame length, and the type of payload carried in the frames. You can also optionally specify the destination, source, sequence, originator exchange, and responder IDs for transmitted frames.

NOTE:

If you change the frame length when the unit is already transmitting traffic, the unit resets your test results, but some residual frames of the old length may be counted if they are already in the traffic stream.

To specify Fibre Channel settings

Step1 If you haven't already done so, use the Test Menu to select the layer 2 terminate test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 Select the **Setup** soft key, and then select the **Fibre Channel** tab.

Step3 In Tx Payload, select one of the following:

– **Acterna.** To transmit frames that contain a sequence number and time stamp so that lost frames and round trip delay can be calculated, select **Acterna**.

If you are measuring round trip delay on a 10 Gigabit circuit, in RTD Setup, indicate whether you want to measure delay with a high degree of precision, or a low degree of precision. In most instances, you should select **High Precision - Low Delay**.

NOTE: You must select an Acterna payload to measure round trip delay and count lost packets. For details, see "Measuring round trip delay" on page 259.

– **BERT.** To transmit frames with payloads filled with the BERT pattern you specify, select **BERT**, and then select a pattern.

Various pseudo-random and Fixed patterns are available. The Pseudo-random patterns continue from one frame into the next. The fixed patterns restart each frame, such that the frame will always start with the beginning of the pattern.

If you set the BERT Pattern to User Defined, in the User Pattern field, specify the 32 bit fixed pattern that will be repeated in the payload.



NOTE:

The Transport Module and Multiple Services Application Module transmit the bytes in user defined patterns from left to right; the FST-2802 transmits the bytes in user defined patterns right to left.

For example, a user defined hexadecimal pattern of 12345678 populates the frame as: 12345678.Using the same hexadecimal pattern, the FST-2802 would populate the frame as 78563412.

Step4 In Frame Length, select one of the listed frame lengths, or select User Defined, and then enter a specific frame length in the USER Frame Length field.

Step5 Under Frame Channel Details, specify the following settings for the transmitted frames:

Settings	Values
D_ID	Type the destination ID of the port the frames will be transmitted to using a 3 byte format.
S_ID	Type the source ID for the port transmitting the frames using a 3 byte format.
SEQ_ID	Type the sequence ID for the frames using a 1 byte hexadecimal format.
OX_ID	Type the originator exchange ID for the frames using a 2 byte hexadecimal format.
RX_ID	Type the responder ID for the frames using a 2 byte hexadecimal format.

Step6 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The frame settings are specified.

Specifying Fibre Channel filter settings

Before transmitting layer 2 traffic, you can specify settings that indicate the expected received payload and determine which frames will pass through the receive filter and be counted in the test result categories for filtered layer 2 traffic. The settings may also impact other results.

For example, the incoming frames must pass the filter to be analyzed for a BERT pattern. Local loopback is also only performed on frames that pass the filter.

To specify Fibre Channel filter settings

Step1 If you haven't already done so, use the Test Menu to select the layer 2 terminate test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 Select the **Setup** soft key, and then select the **Fibre Channel Filter** tab.

Step3 If you want to filter received traffic for a specific destination or source ID, or using routing control, data type, or sequence control criteria, under Frame Channel Details, select the corresponding field, enable the filter, by selecting **Yes**, and then specify the filter value:

Settings	Values
R_CTL	Enter the routing control for filtered frames.

Settings	Values
D_ID	Enter the destination ID for filtered frames.
S_ID	Enter the source ID for filtered frames.
Data Type	Enter the data type for filtered frames.
SEQ_CNT	Enter the sequence ID for filtered frames.

Step4 If you want to filter traffic using payload criteria, select **Data** on the Fibre Channel graphic, and then do the following:

– In Payload Analysis, select **On**.

– To use the Tx BERT pattern as the Rx BERT pattern, in Rx<=Tx, select **On**; otherwise, select **Off**.

– If you are analyzing BERT data, and you turned Rx=Tx Off, specify a BERT pattern.

Step5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

The filter settings are specified.

Specifying traffic load settings

Before transmitting layer 2 traffic, you can specify the type of traffic load the unit will transmit (Constant, Bursty, or Ramp). The settings vary depending on the type of load. When configuring a load, you can specify the bandwidth of the transmitted traffic in 1% increments.

For details on the various loads, refer to “Specifying traffic load settings” on page 64 of Chapter 4 “Ethernet and IP Testing”. Before configuring a traffic load for a Fibre Channel test, simply select a layer 2 Fibre Channel application (instead of an Ethernet application).

NOTE:

When testing from 1Gig, 2Gig, or 4 Gig Fibre Channel interfaces, if you configure the instrument to transmit a constant, bursty, or ramped load of 100%, it is designed to transmit slightly less than 100% traffic (99.90%) as a safeguard against overrunning network elements that can not support 100%. When testing from an 8Gig or 10Gig Fibre Channel interface, the module transmits traffic at 99.996% of the line rate.

If you are certain the elements can support true 100% traffic, select the Allow flooding check box when configuring the Constant load.

Transmitting and analyzing layer 2 traffic

Before you transmit layer 2 traffic, you must specify:

– Interface settings (see “Specifying interface settings” on page 252).

– Frame characteristics of the transmitted traffic (see “Specifying Fibre Channel frame settings” on page 254).

– Frame characteristics used to filter received traffic (see “Specifying Fibre Channel filter settings” on page 255).

– Traffic load settings (see “Specifying traffic load settings” on page 256).

After you specify the layer 2 settings, you are ready to transmit and analyze the layer 2 traffic.

To transmit and analyze layer 2 traffic

Step1 If you haven't already done so, use the Test Menu to select the layer 2 terminate test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 Select the **Setup** soft key, and then select the **Interface** tab to specify settings that control the Fibre Channel interface (see "Specifying interface settings" on page 252).

Step3 Select the **Fibre Channel** tab to specify settings that define the frame characteristics of the transmitted traffic (see "Specifying Fibre Channel frame settings" on page 254).

Step4 Select the **Fibre Channel Filter** tab to specify settings that filter the received traffic based on specified frame characteristics (see "Specifying Fibre Channel filter settings" on page 255).

Step5 Select the **Traffic** tab to specify the type of load the unit will transmit (see "Specifying traffic load settings" on page 256).



NOTE

The Gap/Idle time parameter that rounds to 0.001% in Ethernet applications rounds to the nearest 1% in FibreChannel applications.

Step6 Press **Results** to return to the Main screen.

Step7 Connect the module to the circuit.

Step8 On the Main screen, select the **Laser** button.

Step9 Select **Start Traffic** (for constant or bursty loads) or **Start Ramp** (for ramped loads) to transmit traffic over the circuit.

Step10 Verify that the green Signal Present, Sync Acquired, Link Active, and Frame Detect LEDs are illuminated.

Step11 At a minimum, observe the summary, layer 2 link statistics and counts, layer 2 filter statistics and counts, error statistics, and layer 2 BERT statistics.

You have analyzed layer 2 traffic.

Loopback testing

Loopback testing allows you to transmit traffic from one JDSU test set, and then loop the traffic back through a second unit on the far end of a circuit. For details, refer to Chapter 8 "Loop back Testing".

Transmitting and analyzing patterns

Using the instrument, you can stress the jitter and noise characteristics of 1 Gigabit, 2 Gigabit, 4 Gigabit, and 8 Gigabit Fibre Channel components and systems by transmitting continuous random test patterns (CRPAT), continuous jitter test patterns (CJPAT), and the compliant supply noise pattern (CSPAT). These patterns are always transmitted automatically when you turn the laser on.

To transmit a pattern

Step1 If you haven't already done so, use the Test Menu to select the layer 2 pattern test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 Select the **Setup** soft key. The Setup tab appears.

Step3 Select a pattern:

To…	Select…
Emulate a worst case scenario for deterministic jitter by transmitting frames with a broad spectral content.	**CRPAT**
Stress the timing margins in the received eye by exposing the data sampling circuits to large systematic phase jumps.	**CJPAT**
Emulate a worse case scenario for power supply noise within network transceivers.	**CSPAT**

Step4 Press **Results** to return to the Main screen.

Step5 Connect the module to the circuit.

Step6 On the Main screen, select the **Laser** button.

Step7 Verify that the green SIGNAL LED is illuminated.

Step8 Select **Start Pattern** to transmit the pattern over the circuit.

Step9 At a minimum, observe the test results in the following categories:

- Summary
- Pattern Stats

You have transmitted layer 2 patterns.

Measuring service disruption time

You can use two instruments in an end-to-end configuration to measure the service disruption time resulting from a switch in service to a protect line.

To measure service disruption time

Step1 On the near-end and far end units, if you haven't already done so, use the Test Menu to select the layer 2 terminate test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 On the near-end unit, select the **Setup** soft key, and then select the Traffic tab to configure a constant load of traffic (see "Transmitting a constant load" on page 64).

Step3 If you need to specify other settings for the test on the near-end unit, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

Step4 Connect the units to the circuit.

Step5 On the Main screen, select the **Laser** button.

Step6 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step7 On the near-end unit, do the following:

a Start traffic.

b Clear the service disruption time by selecting the Reset Service Disruption Test button.

Step8 Initiate the switch to the protect line.

Step9 Observe the service disruption result in the Fibre Channel L2 Link Stats category.

Service disruption time is measured.

Inserting errors

Buttons on the Main screen allow you to insert errors into the traffic stream. If you turn on a particular error insertion rate, the error insertion continues even after you restart a test or change the test configuration.

To insert errors

Step1 Select one of the following error types.

- Code
- CRC
- Bit (BERT payload only)

Step2 Do the following:

- Specify the insert type (**Single**, **Burst**, or **Rate**).
- If you specified Burst, enter the quantity of errors in the burst, and then select **OK**.
- If you specified Rate, select the rate.

Step3 Press the **Error Insert** button.

Error insertion starts, and the associated button turns yellow. To stop error insertion, press the button again. Error insertion stops, and the associated button turns gray.

Measuring round trip delay

When you perform loopback tests, you can measure round trip delay by transmitting an Acterna payload. Frames with an Acterna payload carry time stamps, enabling the instrument to calculate the delay.



NOTE:

If you perform an end-to-end Fibre Channel test, invalid delay results appear. You must use a loopback configuration when measuring round trip delay. For details, refer to Chapter 8 “Loop back Testing”.

To measure round trip delay

Step1 If you haven’t already done so, use the Test Menu to select the layer 2 terminate test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 Select the **Setup** soft key, and then select the Fibre Channel tab.

Step3 Under Tx Payload, select an **Acterna** payload. The Acterna payload transmits frames with a time stamp and sequence number. You must select an Acterna payload to measure round trip delay.

Step4 In Frame Length, select one of the listed frame lengths, or select User Defined, and then enter a specific frame length in the USER Frame Length field.

Step5 If you need to specify other settings for the test, select the appropriate tab; otherwise, press **Results** to return to the Main screen.

Step6 Connect the module to the circuit.

Step7 On the Main screen, select the **Laser** button.

Step8 Select **Start Traffic** (for constant or bursty loads) or **Start Ramp** (for ramped loads) to transmit traffic over the circuit.

Step9 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step10 At a minimum, observe the delay test results in the Fibre Channel L2 Link Stats category.

Round trip delay is measured.

Monitoring layer 2 traffic

Use the layer 2 traffic monitor application whenever you want to analyze the received signal. When you configure your test, you can specify settings that indicate the expected received payload and determine which frames will pass through the receive filter and be counted in the test result categories for filtered layer 2 traffic. The settings may also impact other results.



NOTE:

You must turn the laser on using the associated button to pass the signal through the unit's transmitter.

To monitor layer 2 traffic

Step1 If you haven't already done so, use the Test Menu to select the layer 2 monitor/through test application for the interface you are testing (refer to Table 26 on page 250 for a list of applications).

Step2 Select the **Setup** soft key, and then select the **Fibre Channel Filter** tab, and then specify the filter settings for the traffic you want to monitor (see "Specifying Fibre Channel filter settings" on page 255).

Step3 Press **Results** to return to the Main screen.

Step4 Connect the module to the circuit.

Step5 On the Main screen, select the **Laser** button.

Step6 Verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step7 At a minimum, observe the summary, layer 2 link statistics and counts, layer 2 filter statistics and counts, error statistics, and layer 2 BERT statistics test results.

Layer 2 traffic is monitored.

Emission Lowering Protocol

Use the Emission Lowering Protocol (ELP) configuration settings to change the Ordered Sets that will be transmitted during the Link INIT and as fill words after the link goes into the active state.

Depending on the hardware in the network, interoperability may be improved by the use of a different configuration.

ELP configuration

Step1 Select ELP configuration from the Physical Layer subtab of the Interface Tab in the Interface Quick Config settings area.

Step2 Select **Mode.** Then select the combination of Link INIT and Fill Words desired.

- **a** ELP OFF/Disabled - IDLE link INIT and IDLE fill words.
- **b** ELP ON/Enabled IDLE/ARBff - IDLE Link INIT and ARBff fill words.
- **c** ELP ON//Enabled ARBff/ARBff- ARBff Link INIT and ARBff fill word.

12

Automated Testing

This chapter provides information on using the automated scripting programs that are available, depending on the how the unit is equipped and configured. These programs include TrueSAM, J-QuickCheck, Automated RFC 2544, SAMComplete, Fiber Channel, FTP Throughput, HTTP Throughput, TCP Throughput, and the proprietary TrueSpeed sequence of tests that includes a Walk the Window test.

The following topics are discussed in this chapter:

– "TrueSAM" on page 264
– "J-QuickCheck" on page 283
– "Launching a single automated test" on page 279
– "Automated RFC 2544 and Fibre Channel tests" on page 282
– "SAMComplete" on page 304
– "Automated VLAN tests" on page 317
– "Automated FTP Throughput tests" on page 318
– "Automated HTTP Throughput tests" on page 320
– "Automated TCP Throughput tests" on page 321
– "TrueSpeed Test" on page 321
– "Testing using TAM automation" on page 332
– "Saving automated test report data" on page 336

TrueSAM

To assist in the turnup process of a single service, the TrueSAM function provides a simple and complete method to run multiple tests on the system without having to reconfigure each time a test is run. After answering a few prompts, the tests will run automatically, without input from the user, and store the test results in a report.

TrueSAM contains a number of different predefined testing options that are readily available and allows selection of the following automated tests:

- J-Quick Check
- RFC 2544 or SAMComplete
- J-Proof
- TrueSpeed

NOTE: Depending upon how your unit is optioned and configured, your unit may not have all of these options available.

To assist the user in the configuration process, TrueSAM has implemented a Guide Me feature to step through the necessary configuration sequence. This allows technicians with less experience to be able to effectively run the tests for the environment in which they are operating.

To simplify the interface, TrueSAM now provides the complete, interactively linked map of the configuration process as an optional display for the more advanced user. This navigational aid is especially useful when reconfiguring a saved profile.

After configuring the test settings, the setup profile can be saved for future use.

TrueSAM operates with the following constraints

- TrueSAM does not support one-way delay (OWD) measurements.
- TrueSAM is not available for the 40/100G Transport Module.

The following topics are discussed in this section:

- “Setting up TrueSAM” on page 264
- “Loading TrueSAM Profiles” on page 277
- “Running TrueSAM” on page 278

Setting up TrueSAM

Although TrueSAM is a scripting file that runs tests automatically, the appropriate tests (for the circuit being tested) must be selected, and the communications parameters defined, to have the equipment and links between them tested.



NOTE

If it desired that the tests included in this feature be run end-to-end (both local and remote unit running tests) both units will have to be configured and optioned to do so.

TrueSAM Initiation and communication configuration

Step1 From the Test menu, select the interface, and then TrueSAM Terminate.

Step2 The Profile Selection page appears.

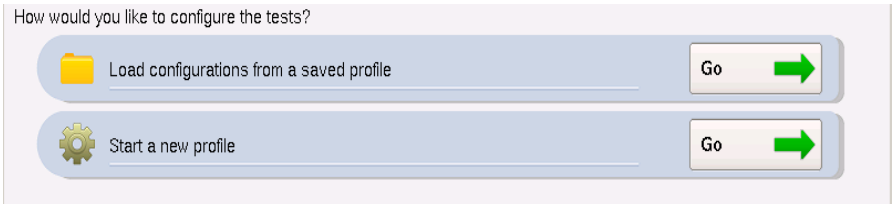


Figure 76 TrueSAM Profile Entry Method Selection

To load configuration settings set from a previously saved file, select **Go (green arrow)** to the right of Load Configuration from a Profile. Go to “Loading TrueSAM Profiles” on page 277.

To configure all options yourself, select **Go (green arrow)** to the right of Start a New Profile. Go to step 3.

Step3 The Operating Layer Select page appears.

Select **Go (green arrow)** after selecting the layer on which your service operates - either **Layer 2** or **Layer 3**.

Step4 After initializing, the TrueSAM main page appears.

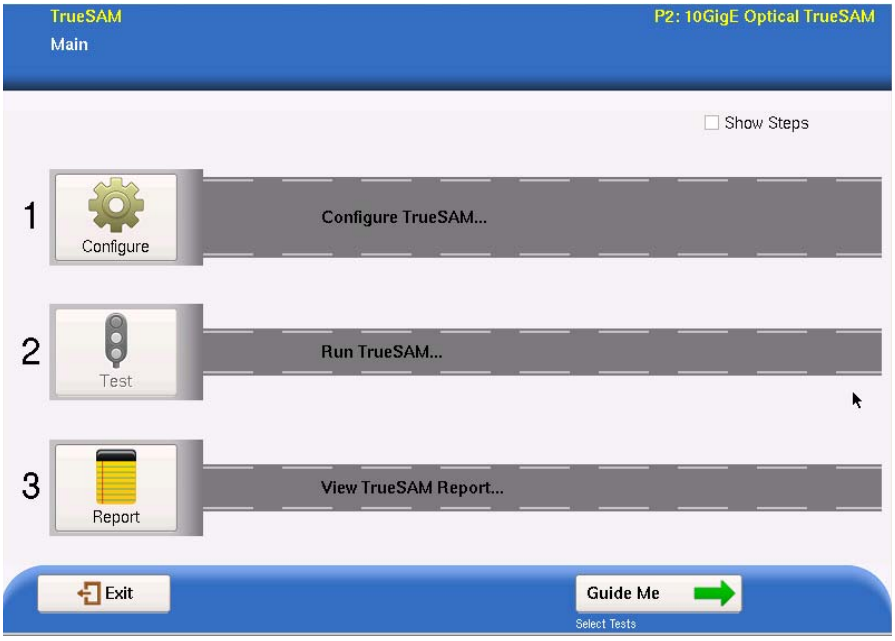


Figure 77 TrueSAM Main Page

This page is used to initiate some of the major actions in the application.

Actions that are not valid at any given time will be grayed out. For example, when the test is first initiated, the Run TrueSAM button will be grayed out because the test has not yet been configured.

To view the component parts of these major actions, the **Show Steps** checkbox can be selected. The configuration steps are displayed and can be used to access these component steps by selecting them (see Figure 78). Configuration steps not applicable for the chosen sequence of tests will be grayed out.

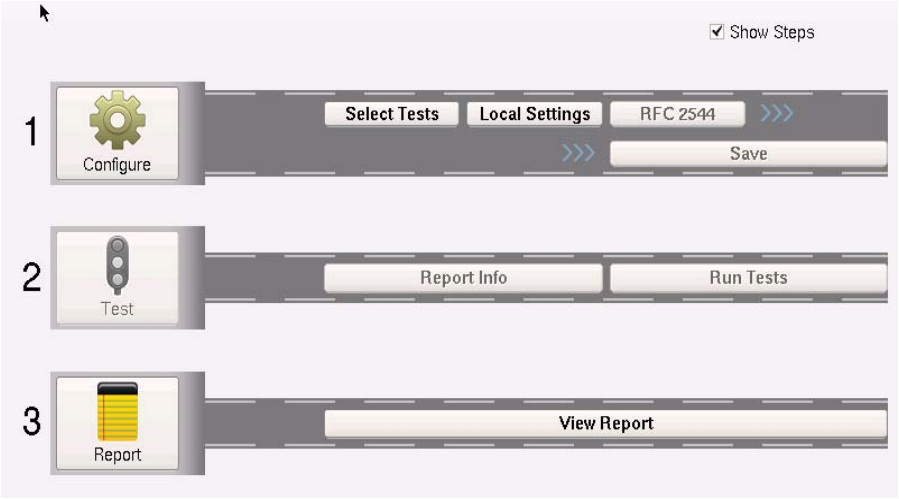


Figure 78 TrueSAM Main Page with Steps shown

From this page you can initiate the following actions:

– Configure TrueSAM. To define all the parameters for the test at this time, select **Configure TrueSAM.** For more information on configuring the TrueSAM tests, go to step 5**.**

– Run TrueSAM. To initiate a configured test script, select **Run TrueSAM**. For more information on running the TrueSAM tests, go to “Running TrueSAM” on page 278

– View TrueSAM Report. To review a detailed report of the results obtained from running the test, select **View TrueSAM Report**. For more information on viewing the TrueSAM reports, go to “Running TrueSAM” on page 278.

– Guided Configuration. To follow a guided path, accessing every applicable page in the configuration and testing sequence, the **Guide Me (green arrow)** may be selected at the bottom of the window. Continue selecting the green arrow at the bottom of every page until the necessary configuration selections have been made and the entire configuration and testing sequence is completed.

Step5 A status screen will momentarily appear with the current action being implemented highlighted in the list. This list will appears at various times while using the TrueSAM application to inform the user of the current action and to indicate to the user actions that are valid. Valid actions will be preceded by a green check mark.

Step6 The Select Tests screen appears.

The following tests are available to be included in the TrueSAM test.

– J-QuickCheck - automatically selected for all users to verify the ability to run other tests.
– Enhanced RFC 2544 - not able to be run simultaneous with SAMComplete. For more information about this test, see “Automated RFC 2544 and Fibre Channel tests” on page 282.
– SAMComplete - not able to be run simultaneous with Enhanced RFC 2544. For more information about this test, see “SAMComplete” on page 304.
– J-Proof - used to verify Layer 2 transparency (layer 2 services only). For more information about this test, see “Using J-Proof to verify layer 2 transparency” on page 74.
– TrueSpeed - used to determine Throughput and Performance of the circuit. For more information about this test, see “TrueSpeed Test” on page 321.

If a test is not applicable for the current configuration it is grayed out.

Select the tests to be included in the TrueSAM test, then select **Next** (the green arrow).

Configuring communications channels

Step1 The Connect Local Settings parameters screen appears.

Specify the communication parameters for the local unit.

a Choose whether the Source MAC address is to be **User Defined** or should the **Factory Default** be accepted.

b For Layer 3 services, select the L3-Source Type - **Static** or **DHCP**.

c Enter the **Source IP**, **Subnet Mask** and **Default Gateway** to be used for this test.

Select **Next** (the green arrow).

Step2 The Connect Channel parameters screen appears.

Specify the channel communication parameters for the remote unit.

– Specify the Encapsulation Method **- None, VLAN** or **Q-in-Q**.
– Specify the FrameType **- DIX** or **802.3**.
– If you selected VLAN, specify the **VLAN ID**.
– Specify the **Interface** connector, if multiple interfaces are available. Select **Details** to access the Interface parameters and change frequency offset or flow control settings.
– Specify the **Destination IP** of the remote unit on the network or select **Help me find the Destination IP** which will scan the subnet for connected IP addresses. After highlighting the desired unit in the list of available units found, select **Use selected**.



NOTE:

If you are testing L3 services and are using DHCP to assign an IP address for the remote unit, communication issues may occur when using TrueSAM. This is because the local end will switch tests on the far end as necessary in order to run the selected tests. This test switching may cause the far end to acquire a new IP address, in which case the near end would not be able to communicate with it anymore. As an alternative, you could try using longer DHCP leases on the far end (so the IP address will be maintained for longer), or use static IP addresses.

To verify that the address entered is accessible, select **Ping**, After address has been confirmed, select **Connect to Channel** to establish communications with the remote unit. After the physical link has been established, the button turns yellow.

NOTE

Upon connection to the remote unit, if there is some form of incompatibility, a message will appear on the screen and make a suggestion to alleviate the situation, e.g., upgrade the software on one of the units. For assistance in this process see “Synchronizing to the StrataSync Server” in the *Getting Started Manual* shipped with this unit.

Select the **right-facing green arrow** at the bottom of the screen.

Configuring RFC 2544 within TrueSAM

The next number of screens are used to configure the RFC2544 test if selected in step 6 “TrueSAM Initiation and communication configuration” on page 264.

Step1 The Symmetry screen appears.

a Select the Throughput type:

Symmetric – used where only one set of throughput parameters are defined because upstream and downstream transmission is identical as the signal is being looped back to the source or transmitted both downstream and upstream.

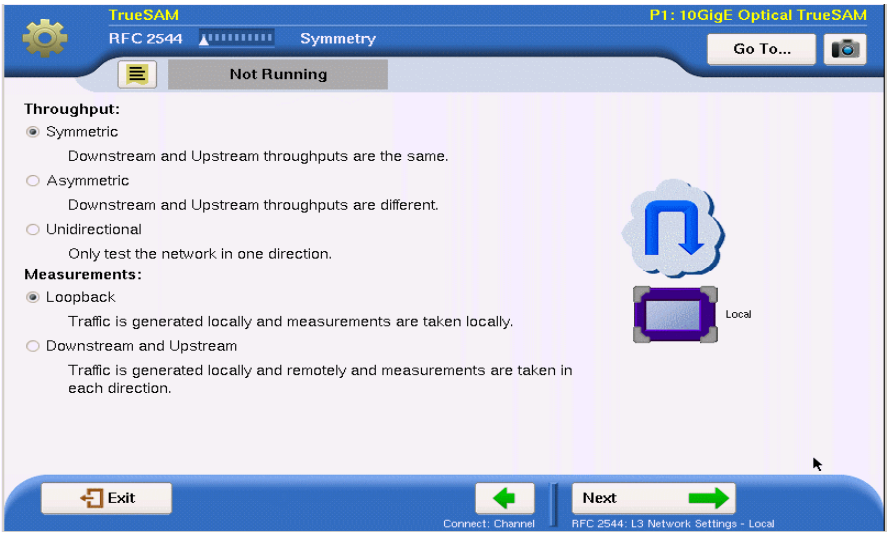


Figure 79 Symmetric Connection - Loopback Option

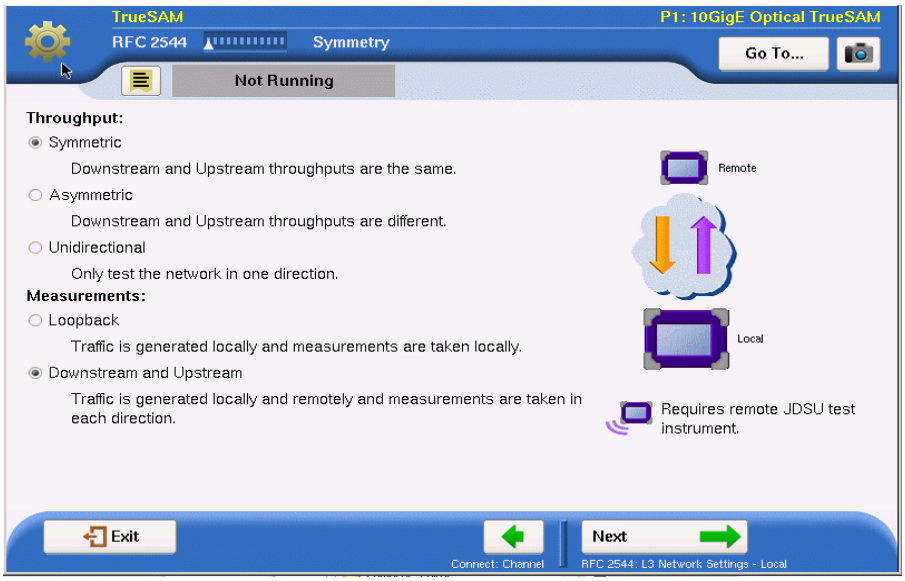


Figure 80 Symmetric Connection- Bidirectional Option

Asymmetric – used where upstream and downstream parameters in a bi-directional test are individually specified and may be different.

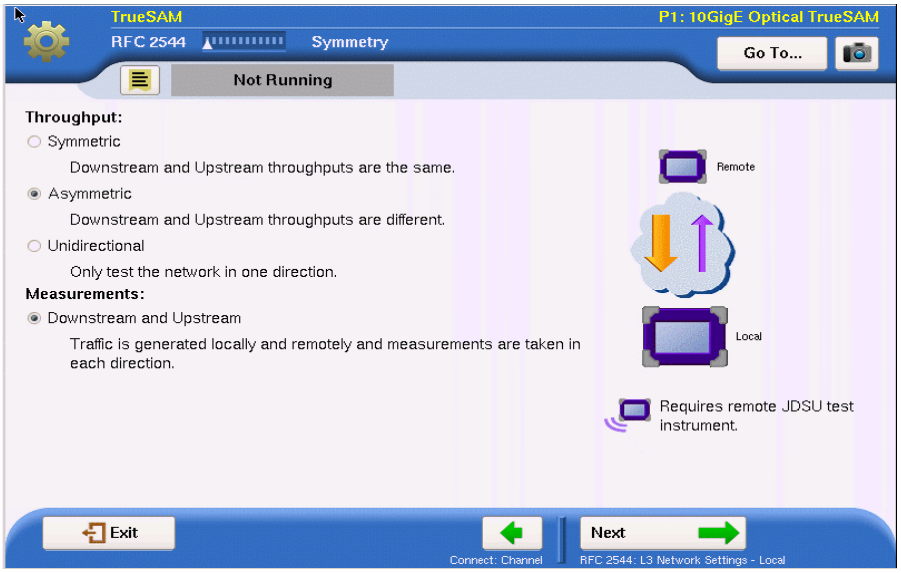


Figure 81 Asymmetric Connection Option

NOTE:

ARP must be enabled on both units if running a bi-directional TrueSAM test in L3 or Wirespeed applications.

Unidirectional – test is only conducted in one direction. May be either upstream or downstream.

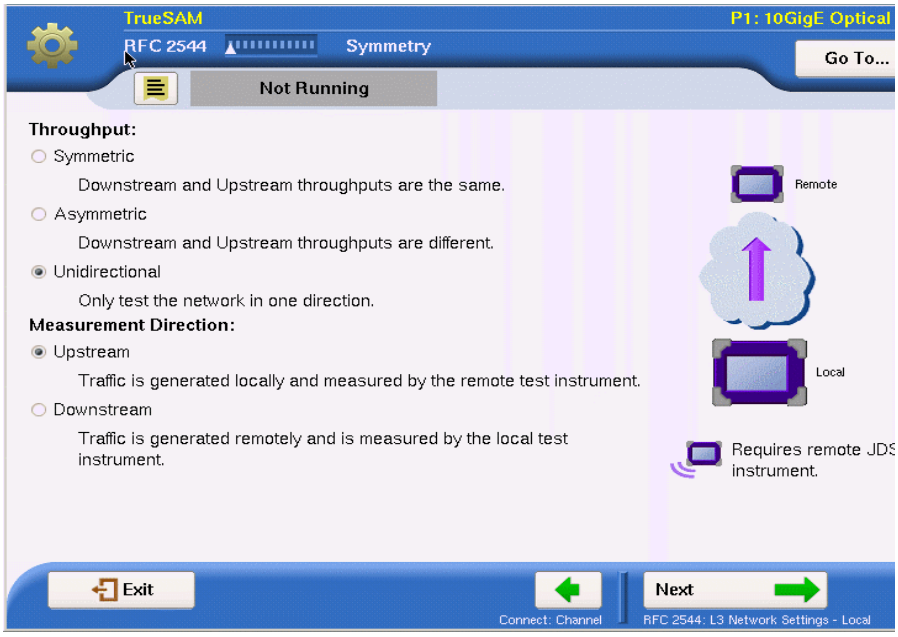


Figure 82 Unidirectional Connection Options

b Depending upon the chosen Throughput Type, select Loop back or One-Way Transmission and Direction, if needed:

– Loop back - only available with Symmetric throughput type as the signal is being looped back to the source, thus identical parameters are required.

– One-Way Transmission - tests are only conducted in a single direction. For Unidirectional Throughput type direction, Upstream or Downstream must be specified.

Note that the diagram on the right of the interface page indicates the type of testing to be done, and indicates if a second JDSU test instrument is required at the remote location.

c Select **Next** (the green arrow).

Step2 If layer 3 testing has been selected, the Local Network Setting screen appears to define the IP prioritization of the Local unit. If layer 2 testing is being done, go to step 4.

a Enter the **TOS** value or

b Select the **DSCP** value.

c To further configure the local network settings select the **Set Time to Live** link at the end of the IP prioritization pane. Set the number of hops constraint and then select the **Back** button (left green arrow).

d Select **Next** (the green arrow).

Step3 The Remote Network Setting screen appears to define the IP prioritization of the remote unit.

a Enter the **TOS** value or

b Select the **DSCP** value

c To further configure the remote network setting select the **Set Time to Live** link at the end of the IP prioritization pane. Set the number of hops constraint and then select the **Back** button (left green arrow).

d Select **Next** (the green arrow).

Step4 The configuration template screen appears allowing the user to select from a number of pre-configured templates to define the parameters to test different types of networks.

a If a configuration template is desired, select the **Yes** radio button.

b Select the desired template from those available in the drop-down box.

c When the selected parameters have been applied, a notice is given. Select OK to return to configuration template screen.

d Select **Next** (the green arrow).

Step5 The Select Tests Window appears to allow the selection of the desired tests to be run. If a configuration template has been applied certain selections will be predefined but all options may be changed, if desired.

a Select or confirm the tests to be run.

b Select **Next** (the green arrow).

Step6 The Utilization window appears to specify the bandwidth parameters- the **Bandwidth Unit** and the **Max Bandwidth** can be selected.

To choose whether the bandwidth units used for the tests are chosen from **Layer 1** or **Layer 2**, make the selection in the Bandwidth Unit drop-down box. Then enter the **Max Bandwidth (in Mbps)** in the entry box (Upstream and/or Downstream for non-symmetric test).

To further refine the Utilization configuration, select **Set advanced Utilization settings** and then select **Allow True 100% Traffic**, if desired. Select **Back** to return to previous screen.

Select **Next** (the green arrow).

Step7 The Frame Lengths screen appears to allow the definition or confirmation of the frame or packet length parameters,

a Select whether the length type of **Frames** or **Packets**.

b Select the number of frame or packet lengths to be tested by checking the appropriate number of boxes and then entering a value for each checked Upstream and/or Downstream (depending on the symmetry selection) Frame or Packet length to be tested.

c Select **Next** (the green arrow).

Step8 If selected, the Throughput Test screen appears to allow selection or confirmation of the throughput parameters.

a Select or confirm whether the **RFC 2544 Standard** or the **JDSU Enhanced** zeroing-in process is to be used.

b Confirm or define the **Measurement Accuracy** from the drop-down box values.

c Select **Next** (the green arrow).

Step9 If selected, the Frame Loss Test screen appears to allow configuration of the parameters necessary for the Frame Loss Test.

a Select the desired Test Procedure from these options -

RFC 2544. Transmits traffic at the maximum bandwidth, and then decreases the bandwidth for each trial by the granularity you specify. The test ends after two successive trials with no frames lost. This procedure also requires specification of **Bandwidth Granularity** in Mbps**.**

Top Down. Transmits traffic at the maximum bandwidth specified in the **Test Range** setting, and then decreases the bandwidth for each trial by the **Number of Steps** specified until the minimum bandwidth is reached for the specified Test Range.

Bottom Up. Transmits traffic at the minimum bandwidth specified in the **Test Range** setting, and then increases the bandwidth for each trial by the **Number of Steps** specified until the maximum bandwidth is reached for the specified Test Range.

b To further refine the frame loss configuration, select **Set advanced Frame Loss measurement settings** and then choose to **Measure Packet Jitter** by selecting the checkbox, if desired. Select **Back** to return to previous screen.

c Select **Next** (the green arrow).

Step10 If selected, the Back to Back Test screen appears to define the parameters for the Back to Back test

a Set the **Max Burst Duration** (Upstream and/or Downstream for non-symmetric test) of each test and **Burst Granularity** in Frames (L3).

b To further refine the Back to Back test, select **Set advanced Back to Back settings** and then choose the **Ignore Pause Frames** checkbox. Select **Back** to return to previous screen.

c Select **Next** (the green arrow).

Step11 If selected, the Burst Test screen appears to allow the confirmation or configuration of the Burst Test parameters

a Select the Burst Test Type - either **Committed Burst Size (CBS)**, **CBS Policing (MEF 34)** or **Burst Hunt**

b Define the **CBS (in kB)** (Upstream and/or Downstream for non-symmetric test), **CBS Duration** and **Burst Sizes (kB**) (Upstream and/or Downstream for non-symmetric test) depending on which Burst test type is chosen.

c To further refine the Burst Test, select **Set advanced CBS settings** and then select the **Ignore Pause Frames** checkbox, if desired. Select **Back** to return to previous screen.

Step12 The Test Durations screen appears for specification of whether all tests are to have common durations or are individual tests to have their durations specified separately.

a To choose common durations, select or confirm the **No** radio button. If individual setting are desired, select or confirm the **Yes** radio button.

b Specify or confirm the **Durations** and the **Number of Trials** for all tests.

c Select **Next** (the green arrow).

Step13 The Test Threshold screen appears to allow setting of the pas/fail threshold for the selected tests.

a Place a check mark in the box in front of the each test where a pass/fail threshold is desired.

b Enter or confirm the threshold value in the entry box after the test name.

c Select **Next** (the green arrow).

All RFC 2544 tests have been configured.

– If doing layer 2 testing and J-Proof has been selected, got to “Configuring J-Proof test within TrueSAM” on page 273.
– If TrueSpeed test has been selected, go to “Configuring TrueSpeed tests within TrueSAM” on page 274.
– If TrueSpeed test has not been selected, go to “Saving TrueSAM profile” on page 276.

Configuring SAMComplete test within TrueSAM

The configuration of the SAMComplete test initiated from within TrueSAM is nearly identical to that for the standalone SAMComplete test. The configuration of the TrueSAM version can be accomplished by starting on step 2 of “Configuring SAMComplete test settings” page 307 with one exception - the local and remote connection settings (step 5 and step 6) will have already been configured by J-QuickCheck. Skip to step 7 and continue.

After SAMComplete configuration step 11has been completed, return to this point in the TrueSAM configuration procedure.

– If doing layer 2 testing and J-Proof has been selected, got to “Configuring J-Proof test within TrueSAM” on page 273.
– If TrueSpeed test has been selected, go to “Configuring TrueSpeed tests within TrueSAM” on page 274.
– If TrueSpeed test has not been selected, go to “Saving TrueSAM profile” on page 276.

Configuring J-Proof test within TrueSAM

If layer 2 testing is being done and the J-Proof test has been selected, the J-Proof frames screen appears. By default, a single test frame appears in the frame list. You can specify a name for the frame, the control protocol format, the number of frames of this type to transmit (the count), the frame rate, and the time-out period.

Step1 To modify the settings for the transmitted frame:

a If you want to name the frame, select **Test Frame** in the Name column and then enter a name of up to twenty characters on the pop-up keypad or the remote keyboard. Select **OK** to close the keypad and store the name.

b In the **Protocol** column, select the control protocol format for the frame from the drop-down options.

c In the **Count** column, specify the number of frames you want to transmit.

d In **Rate (fr/sec)** column, enter the rate at which you want to transmit the frames.

e In **Time-out (msec)** column, enter the number of milliseconds the instrument will wait to receive the looped back frame before stopping transmission of frames.

Step2 If you want to transmit control frames for different protocols, do one of the following:

– Select the **Add Frame** soft key. Specify the settings listed in step 1.Repeat this step for each type of frame desired. Select **Remove frame** to remove the highlighted frame from the list

or

– Use the **Quick Config** soft key populate the frame list with a group or all protocol control frame types. See “Using Quick Config to configure test frames” on page 76 for more information.

Step3 Select **Next** (the green arrow).

The J-Proof test within TrueSAM is configured.

– If TrueSpeed test has been selected, go to "Configuring TrueSpeed tests within TrueSAM" on page 274.

If TrueSpeed test has not been selected, go to "Saving TrueSAM profile" on page 276.

Configuring TrueSpeed tests within TrueSAM

The next two screens are used to configure the TrueSpeed test within TrueSAM, if selected in step 6 of "TrueSAM Initiation and communication configuration" on page 264.

Step1 The first screen allows for the setting or confirmation of how the throughput is to be configured.

a If it is desired to obtain throughput parameters from the RFC 2544 test, **Set Bottleneck Bandwidth to match RFC 2544 Max Bandwidth when loading TrueSpeed configuration** is checked, and other throughput options are grayed out.

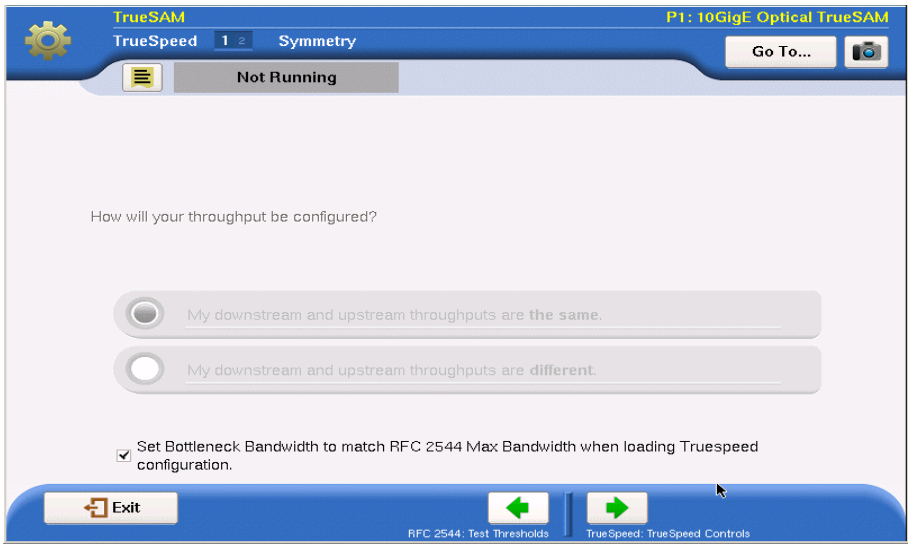


Figure 83 TrueSAM TrueSpeed throughput definition

NOTE:

Use the **Set Bottleneck Bandwidth to match RFC 2544 Max Bandwidth** setting when the bandwidth is L1/L2 Mbps or L1/L2 Kbps.

b If throughput parameters are not obtained from the RFC 2544 test, select either **My downstream and upstream throughputs are the same** or **My downstream and upstream throughputs are different.**

c Select **Next** (the green arrow).

Step2 The next screen provides for the configuration of the parameters pertaining to the Committed Information Rate (CIR) and TCP Threshold.

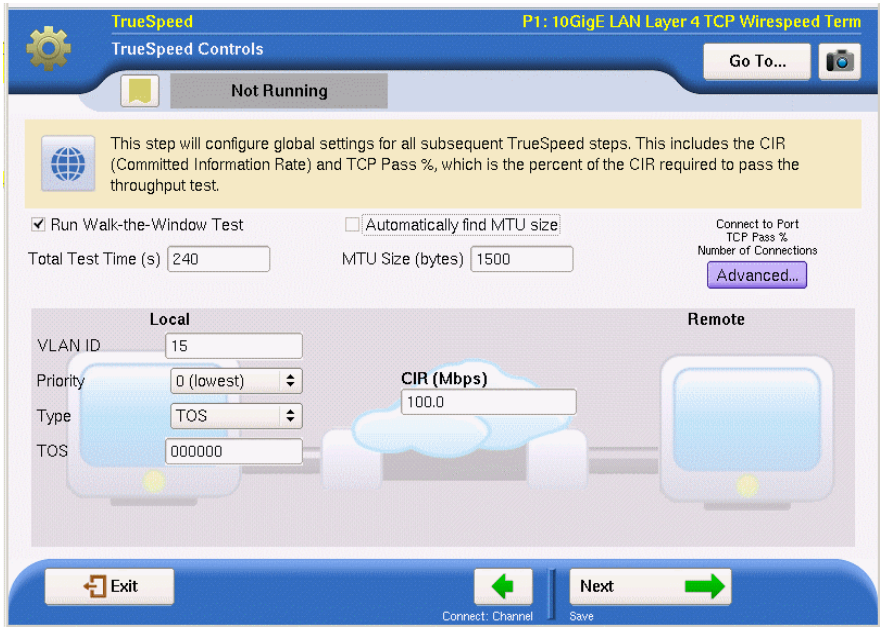


Figure 84 TrueSpeed Symmetrical Turnup Configuration

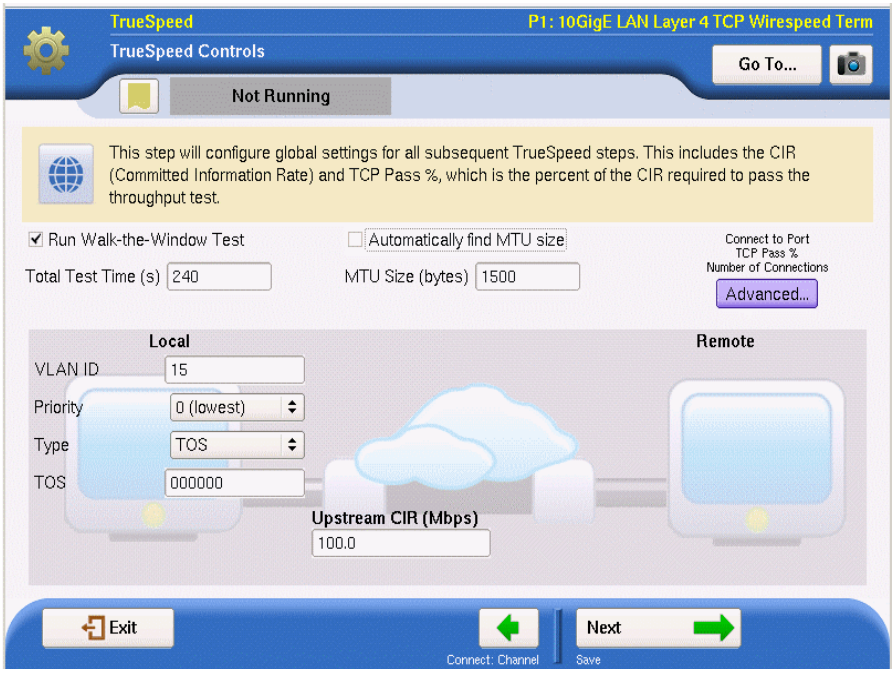


Figure 85 TrueSpeed Asymmetrical Turnup Configuration

a Specify or confirm whether to **Run the Walk the Windows Test** by selecting the checkbox.

b Specify or confirm whether to **Automatically find MTU size** by selecting the checkbox. If not checked, enter the desired **MTU Size** in bytes.

c Enter or confirm the IP Prioritization for both the local and remote end, if necessary. Select **TOS** and enter the value or select **DSCP** and enter its value.

d Enter or confirm the **CIR** in Mbps. This will be unavailable for entry if Set Bottleneck Bandwidth to match RFC 2544 Max Bandwidth when loading TrueSpeed configuration was checked on previous screen.

e To further configure the remote network setting select the **Advanced** button. Define the **Port Connection**, **TCP Pass %,** the **MTU Upper Limit** (in bytes) and whether **Multiple Connections** are desired. When these have been defined, select **Back** (left green) arrow.

f After all parameters have been specified, select **Next** (the green arrow).

Saving TrueSAM profile

The Save Profile window appears.

Step1 Do one of the following:

– If no Profile is to be saved at his time, select **Next** (the green arrow). Go to step 2.

– If it is desired that the configuration be saved to memory (disk or USB), specify the filename.

a To save somewhere other than the default location, press the **Select** button after the filename to define the directory where it is to be stored.

b If it is desired that subsequent users be restricted from being able modify this profile (may be modified if saved under different filename), check the box **Save as read-only**.

c To save the file to memory, select the **Save Profiles** button. Then select the **Next** (the green arrow).



NOTE

Any TrueSAM profile saved from BERT software prior to v.17 is not compatible with the subsequent versions of the application. These profiles must be re-configured and saved again to remove the incompatible settings.

Attempts to configure a unit with a TrueSAM application in BERT software older than v.17 with profiles saved on a current unit (transferred on USB stick, over network, etc.) will also be unsuccessful.

Step2 The TrueSAM Edit/Run screen appears.

Go to step 4 of"TrueSAM Initiation and communication configuration" on page 265.

Loading TrueSAM Profiles

Test profiles that configure all parameters of TrueSAM may have been previously saved into the memory. These tests can be loaded and run without any changes or may be used as templates where any number of parameters may be modified after loading.

NOTE

Any TrueSAM profile saved from BERT software prior to v.17 is not compatible with the subsequent versions of the application. These profiles must be re-configured and saved again to remove the incompatible settings.

Attempts to configure a unit with a TrueSAM application in BERT software older than v.17 with profiles saved on a current unit (transferred on USB stick, over network, etc.) will also be unsuccessful.

If you load a profile that was configured on another unit, and that profile specified including a logo in the test report, make sure that the .png, .jpg, or .jpeg is in the following folder on your unit: `/acterna/user/disk/bert/images`

Loading profile from memory

The Profile selection window appears.

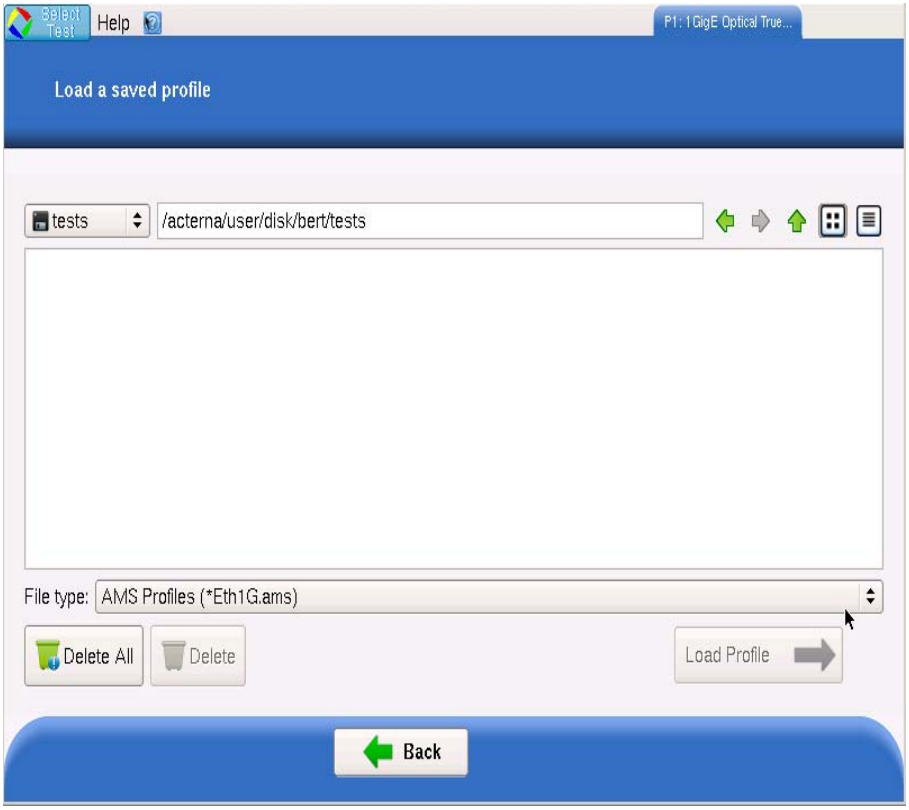


Figure 86 Saved Profiles window

The filenames of the saved profiles will be listed in the center of the window.

Do the following:

Step1 The default display will be of saved profiles for the currently selected interface. To select a configuration saved from another interface, select from the drop-down list accessible by clicking on the up-down arrow at the right end of the File Type field displayed under the files list window.

Step2 To manage files on the displayed list, select the desired file(s) and then select the **Delete** or **Delete All** buttons to remove them from the memory.

Step3 To load a profile, select one from the list whose configuration is to be loaded.

Step4 Select the **Load Profile** button to load the configuration for all tests. After profile has successfully loaded select, **OK** and then select **Next** (the green arrow).

The TrueSAM profile has been loaded.

Step5 The TrueSAM Edit/Run screen appears.

– To change the configuration, go to step 4 of "TrueSAM Initiation and communication configuration" on page 266.

– To run the test, go to "Running TrueSAM" on page 278

Running TrueSAM

After specifying settings or loading a profile, you are ready to run the test.

To run TrueSAM

Step1 Select **Run tests**.

Step2 The report info screen will display.

This screen allows the user to enter information about the test which will be added to the report that is automatically generated as the test is run.

This information includes-

Customer Name

Technician ID

Test Location

Work Order

Comments/Notes

Custom Logo (from memory)

Step3 After all the desired data is entered into the entry boxes, select **Next** (the green arrow).

Step4 A number of screens will appear providing data about how the test is configured. If everything appears as desired, select **Next** (**right-pointing green arrow**) until it displays the Run Tests button on the bottom of the screen. Select **Run Tests.**

Step5 As the test are running, an overall result view, including screen shots of the various tests, is available and shows real-time status of the tests as they execute. The test displays a green (Passed) or Red (Failed) banner at the top of the screen when the test is completed.

When all test are completed, the report is automatically generated and saved to memory.

Select the **Next** (the green arrow).

The TrueSAM Edit/Run/View screen appears. Go to step 4 in "TrueSAM Initiation and communication configuration" on page 265.

Launching a single automated test

The TrueSAM application is ideal for service turn-ups. But, if the service is already functioning and a specific problem needs to be examined, there are automated tests that can be run individually.

There are two ways to launch automated test scripts from the Test Select application and the automated script in which it is to be run.

– Directly from the Select Test menu, for example by choosing Ethernet, then the line rate 1GigE Optical, then the automated test RFC 2544, then the layer L2 Traffic and then the port P1 Terminate.
– From within a base application, such as “1GigE>Layer 2 Traffic> Term”, specifying the automated test to be run by a soft key on the right side of the interface, or by a button inside the Toolkit which is opened by the Toolkit softkey. Note that all toolkit functions are also provided in the Tools menu (depending on your model, accessed from the menu bar along the top of the interface, or from the Tools icon in the lower-left corner.)

In most cases, the relevant configuration settings are available within the automated test, but if the base application configuration must be changed before running the automated test, use option 2 above to launch the base application, then make the necessary configuration changes, then launch the automated test. You may also use the ‘Load Test…’ menu choice to configure the base application from a Saved Test file before starting the automated test.

To launch from the Select Test menu

Step1 From the Select Test application tree, select the technology and interface desired. All the applications available for the current configuration of the unit will be displayed.

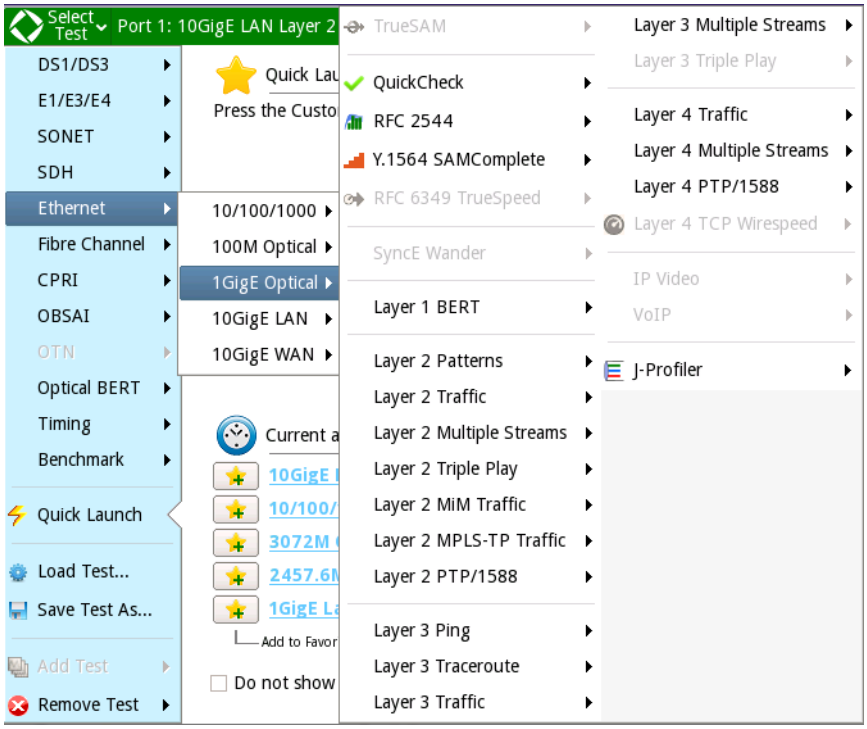


Figure 87 Select Test application tree

Step2 Select the automated script from the top levels of the tree, then the specific test desired. The automated script is launched.

To launch for later use

Step1 Select the technology and interface desired. All the applications available for the current configuration of the unit will be displayed. (See Figure 87 above).

Step2 Select the base application (from the lower part of the application tree) and then initiate the desired automated script using the on-screen soft key on the right side of the interface.

The automated script will be launched, ready to be configured.



NOTE

The Quick Launch window displays previously run and/or saved configurations of applications. Automated scripts launched simultaneously with base applications are fully identified with the script.

To launch from a running application

Step1 If you haven't already done so, use the Test menu to select the appropriate application. Be certain to select **Terminate** or **Dual Terminate** mode.

Step2 Connect the modules on the near-end and the far end to the circuit.

Step3 If you are testing an optical interface, on both units, select the **Laser** button to turn the laser on.

Step4 On both modules, verify that the green Signal Present, Sync Acquired, and Link Active LEDs are illuminated.

Step5 If you are running the test with layer 3 traffic, and you enabled ARP, observe the Message Log to verify that ARP successfully determined the destination MAC address.

Step6 On the Main screen, do one of the following:

- If you are running the RFC 2544 test, press the **Enhanced RFC 2544 Test** soft key, and proceed to "Configuring the Enhanced RFC 2544 or Fibre Channel tests" on page 291.
- If you are running the automated Fibre Channel test, press the **FC Test** or **Enhanced FC Test** soft key, and proceed to "Configuring the Enhanced RFC 2544 or Fibre Channel tests" on page 291.
- If you are running the automated multiple Ethernet service verification SAMComplete test, press the **SAMComplete** soft key, and proceed to "SAMComplete" on page 304.
- If you are running the FTP Throughput or HTTP Throughput automated test, press the press the **Toolkit** soft key, and then select the test you want to run from the Select Tool menu. Proceed to "Throughput test" on page 285 or "Automated HTTP Throughput tests" on page 320.
- If you are running the TCP Throughput automated test, press the **Toolkit** soft key, and then select TCP Throughput. Proceed to "Running TCP Host or Wirespeed applications" on page 158 of Chapter 6 "TCP/UDP Testing".

The automated test is launched.

Automated Test Availability

Table 28 lists the available automated tests for each application.

Table 28 Automated Tests

Automated Test	Application[a]
QuickCheck	Ethernet – Layer 2 Traffic – Layer 3 Traffic
Enhanced RFC 2544 Test	Ethernet – Layer 2 Traffic – Layer 3 Traffic – Layer 4 Traffic
FC Test	Fibre Channel – Layer 2 Traffic
SAMComplete (not applicable with 40G/100G Transport Module)	Ethernet – Layer 2 Traffic – Layer 2 Multiple Streams – Layer 3 Traffic – Layer 3 Multiple Streams – Layer 4 TCP Wirespeed
VLAN	Ethernet – Layer 2 Traffic – Layer 3 Traffic – Layer 4 Traffic
FTP Throughput	Ethernet – Layer 3 Traffic – Layer 4 Traffic
HTTP Throughput	Ethernet – Layer 3 Traffic – Layer 4 Traffic
TCP Throughput	Ethernet – Layer 2 Traffic – Layer 3 Traffic – Layer 4 Traffic
RFC 6349 TrueSpeed Test	Ethernet – Layer 4 TCP Wirespeed

a. The RFC tests are not available when running NextGen GFP or OTN applications.

When running a script in Dual Terminate mode, you can only launch a script for one port. You can not run scripts from both ports.



CAUTION: CORRUPTED RESULTS

Pressing Restart during a test could corrupt the results. To ensure accurate script results, wait for the script to complete before pressing Restart.

Automated RFC 2544 and Fibre Channel tests

If your instrument is configured and optioned to do so, you can use it to run tests that automate the procedures recommended in RFC 2544 for layer 2 Ethernet, layer 3 IP, or layer 4 TCP/UDP (N/A 100G Ethernet Client in OTU4). You can also run a test that uses similar parameters for layer 2 Fibre Channel. The tests prompt you to select key parameters for throughput, round trip delay, frame loss rate, and back to back frame tests, run the tests, and then automatically generates a text file of results for the tests and a log file detailing the progress of the script. A PDF file is also generated which includes the test results in tabular and graphical formats.

The following topics are discussed in this section:

– "Features and capabilities" on page 282
– "About loopbacks" on page 283
– "J-QuickCheck" on page 283
– "Asymmetrical tests" on page 285
– "Throughput test" on page 285
– "Latency (RTD) test" on page 287
– "Packet Jitter test" on page 288
– "About the System Recovery test" on page 288
– "Frame Loss test" on page 289
– "Back to Back Frames test (Burst test)" on page 289
– "Optimizing the test time" on page 290
– "Importing and exporting RFC config files" on page 290
– "Configuring the Enhanced RFC 2544 or Fibre Channel tests" on page 291
– "Specifying the external test settings" on page 292
– "Setting Connection parameters" on page 293
– "Test selection" on page 296
– "Running Enhanced RFC 2544 and FC tests" on page 298

Features and capabilities

The instrument supports the following features when running the RFC 2544 tests:

– Support for all Ethernet line rates and ethernet clients of 11.1G OTN rate layer 2 traffic.
– J-QuickCheck—Before running the Enhanced RFC 2544 test, you can run the J-QuickCheck application to verify that the local and remote instruments are configured properly to bring up the link, verify auto negotiation of the link, establish the link, establish a loop back, and then verify that the link can support 100% traffic utilization. There is also an extended Layer 2 traffic test useful for quick turn-ups. For details, see "Asymmetrical tests" on page 285.
– Graphical output of key results. When running the tests, frame loss, throughput, and latency (round trip delay) results are now displayed graphically in their own result categories.
– Status bar. A status bar is also provided that lets you know how far the test has progressed, and provides an estimate of the time remaining to run the test.
– Report output. You can save the test results to a user-named file in PDF, XML, or TXT format.
– Enhanced test. You can run the Enhanced RFC 2544 test, and indicate whether you want to run a symmetrical test, or an upstream, downstream, or combined asymmetrical test.

– Asymmetric RFC 2544 (not applicable with 40G/100G Transport Module). You can run the Enhanced RFC 2544 test in asymmetric mode in an end-to-end configuration. This is useful for testing circuits carrying traffic at different upstream and downstream line rates. The test is initiated by a master tester (on the near end). The master tester then automatically configures the slave tester on the far end.
– TAM (Test Access Management) automation—If your instrument is configured and optioned to do so, you can now use it to remotely log into and provision network elements (for example, switches and routers) from a Mobility Switching Center (MSC) by issuing TL1 commands. For details, see "Testing using TAM automation" on page 332.
– System recovery testing per RFC 2544 (not applicable with 40G/100G Transport Module). You can use the instrument to determine the amount of time it takes for a network element to recover from a state where it is dropping frames.
– Exporting and importing of configurations for the Enhanced RFC test.
– The Enhanced RFC tests supports both round-trip delay (RTD) and one-way delay (OWD). If your instrument is optioned and configured for one-way delay, you can choose whether to run a Latency (RTD) or Latency (OWD) test.
– TCP Wirespeed test. This is a 5-step test to analyze TCP throughput for 64 connections.

About loopbacks

During the automated tests, the instrument checks for a loopback. It could be one of the following types:

Active loop — the destination has responded to a loop command.

Hard loop — the source and destination addresses are the same for both the returned frames and the outgoing frames.

Permanent loop — the source and destination addresses are switched in the returned frames. Permanent loop is not available L2 or in L3 when ARP is disabled.

J-QuickCheck

The J-QuickCheck application is used to verify that the local and remote instruments are configured properly to bring up the link, verify auto negotiation of the link, establish the link, establish a loop back, and then verify that the link can support 100% traffic utilization.

There are a number of ways in which the J-QuickCheck test may be initiated:

– launch QuickCheck directly from the Test menu (If you are testing 10/100/1000M Electrical, 1GE Optical, 100M Optical, 10GE LAN, 40GE, 100GE. Layer 2 Single Stream TERM or Layer 3 Single Stream TERM, you can launch directly from the Test menu, For example: Tests>10GE LAN>QuickCheck.)
– relaunch Quick-Check from an underlying L2 or L3 traffic application via the Quick-Check button on the right side of the screen.
– the original simple verification that the local and remote instruments are configured properly to bring up the link accessed through the Quick Check button in the tool kit.
– an extended Layer 2 Turnup test
– an automatic initiation of the full RFC 2544 test upon completion of the J-QuickCheck test link verification utilizing maximum throughput rates determined by the J-QuickCheck test

These options can be run in combination or separately.



NOTE:

After specifying settings for QuickCheck in the standalone QuickCheck test (from the Test menu), you may return to the main app if desired, but you should not change any settings or you must change them back before re-entering QuickCheck. Running the test with settings different than originally set may result in some unexpected errors or failures. To restore test defaults, select restore test to defaults or manually restore any settings that were changed.

Understanding the J-QuickCheck stages

At each of the three stages of the J-QuickCheck application, the instrument automatically performs certain actions. Some actions must occur before others can take place. For example, the local port must be up before a loopback can take place.

Local Port

If application for an optical circuit indicates that the local port is down, (indicated by a red **Not Connected** button), verify that the laser is ON on both near and far end instruments. If the application is for an electrical circuit, verify that frame sync and link LEDs are illuminated on both instruments.

Auto-negotiation

Auto-negotiation can not take place until the physical link is established (indicated by a green **UP** button for the local port). If the local port is UP, during the auto-negotiation stage, the instrument does the following:

– If the near end instrument determines that the far end instrument advertises that it supports auto-negotiation, the near end instrument automatically turns auto-negotiation ON, and indicates the negotiated speed and duplex capabilities.
– If you are running the application on an electrical circuit, and the near end instrument determines that the far end instrument does not support auto-negotiation, the near end instrument automatically turns auto-negotiation OFF, sets the duplex setting to FULL, and the line rate to the detected speed. A warning also appears informing you that it's possible the far end port is in half duplex mode.
– If you are running the application on an optical circuit, and the near end instrument determines that the far end instrument does not support auto-negotiation, the near end instrument automatically turns the laser OFF, turns auto-negotiation OFF, then turns the laser back ON. It then indicates the speed and duplex settings.

If at any time during this phase the link or frame synchronization is lost, the instrument will alert you, and will then restart the application automatically.

Remote Loop (traffic test mode)

A remote loop up can not take place until the physical link is established and auto-negotiation succeeds (is either ON or OFF). The instrument sends a loop down, followed by a loop up. If the second attempt fails:

– If running a Layer 2 test (in traffic test mode):

  The instrument checks for a hardware loop. If a hardware loop is not found, it then checks for a permanent loop. If a permanent loop is not found, the instrument declares "No Loop Found".
– If running a Layer 3 or 4 test:

The instrument checks for a permanent loop. If a permanent loop is not found and if ARP is Disabled, the instrument checks for a hardware loop. If a hardware loop is not found, the instrument declares “No Loop Found”. If ARP is Enabled, the instrument declares “No Loop Found”. If all three attempts fail, verify that the correct destination address or port is specified in your application settings, then run the J-QuickCheck application again.

Remote Loop (LBM/LBR test mode)

A remote loop up can not take place until the physical link is established and auto-negotiation succeeds (is either ON or OFF). After link and negotiation have been satisfied, the unit attempts a LBM/LBR loop. If established, the Load Test and Throughput will run. If a LBM/LBR loop is not established, the Remote Loop and Basic Load Test indicators will turn red indicating a failed test.

Basic Load Test

The load test can not take place until a remote loop is established or detected. If a loop is in place, the near end instrument automatically transmits a full load of traffic (100% at the selected line rate) using the frame or packet size that was specified for the application. The instrument then calculates the average layer 2 bandwidth utilization, and displays it as a percentage.

Test at configured Max Bandwidth

With this option selected, the RFC 2544 test will automatically be run upon completion of the J-QuickCheck test using the Max Bandwidth setting pre-configured on the Setup-All Tests tab.

This option may both be selected simultaneously with the “Layer 2 Quick Test”.

Layer 2 Quick Test

The Layer 2 Quick Test extended test option operates in the symmetric, loopback mode only thereby eliminating the number of configuration options. The test can be configured to set the length of time the test is to be run and to configure the CIR in the RFC 2544 settings with a percentage of the Throughput value detected. The default value will be 100% (i.e. CIR will be 100% of the JQuick-Check Throughput).

This option may both be selected simultaneously with “Test at configured Max Bandwidth”.

Asymmetrical tests

When testing upstream and downstream circuits at different line rates, you must run an asymmetric RFC test. Two JDSU Ethernet test instruments must be used at each end of the circuit. One test instrument operates as the master instrument, and executes the RFC test. The other instrument operates as a slave instrument, and is controlled remotely by the master instrument.

Throughput test

The throughput test is used to determine the highest possible bandwidth at which no frames are lost.

JDSU zeroing-in method

The JDSU zeroing-in method functions as follows:

Attempting Phase

- The test starts transmitting traffic at the Maximum Bandwidth, then waits 3 seconds.
- The test does a restart, then waits 5 seconds.
- The test calculates the average layer 2 bandwidth utilized (L2 Avg. % Util).
- If the Bandwidth Accuracy is 1% and the L2 Avg. % Util is less than 99.98%, the throughput is the integer value of the measurement. Otherwise, throughput is 100%.
- If the Bandwidth Accuracy is .1% or .01%:
  - For 1Gig, the test increases the load 3% over the L2 Avg. % Util measured above.
  - For 10 Mb, the test increases the load 30% over the L2 Avg. % Util measured above.
  - For 100 Mb, the test increases the load 3% over the L2 Avg. % Util measured above, or to 100%, if the above increase would exceed 100%.
- If the Bandwidth Accuracy is .1% or .01%:
  - Start traffic at the rate calculated above
  - Wait 3 seconds
  - Do a test restart
  - Wait 5 seconds
  - Get the L2 Avg. % Util

For .1% accuracy, Throughput is calculated as:

- The (integer value of L2 Avg.) % Util * 10 divided by 10

For .01% accuracy, Throughput is calculated as:

- The (integer value of L2 Avg.) % Util * 100 divided by 100



NOTE:

The minimal throughput values for mismatched (asynchronous) rates are 100k to 10G. Anything below 100k (such as 10k) that comes into a 10G unit will not be detected because it is below the threshold granularity supported. (0.001% of 10G = 100k)

Verifying Phase

The load is set to the calculated throughput value, and transmitted for the Throughput Duration time. If the frame loss tolerance is exceeded, instructions are provided for testing the link manually for intermittent problems, and the test is aborted.

Throughput test results

The following results are reported for every frame length selected.

Cfg Length (Mbps)

The bit rate for transmitted traffic (expressed in Mbps) at which no frames were lost for a particular frame length.

Measured Rate (Mbps)

The measured bit rate (expressed in Mbps) at which no frames were lost for a particular frame length.

Measured Rate (%)

The bit rate (expressed as a percentage of the line rate) at which no frames were lost for a particular frame length.

Measured Rate (frms/sec)

The peak frame rate (expressed in frames per second) at which no frames were lost for a particular frame length.

Pause Detected

Indicates whether or not pause frames were detected at the point where no frames were lost for a particular frame length.

These results are also reported when you run the Latency and Packet Jitter tests.



NOTE:

If J-Quick Check is not performed, the report may show loop type achieved.

Pass/fail threshold

You can configure the test to optionally indicate whether the Throughput test passed or failed. To do so, you specify the bandwidth for the Throughput Pass Threshold. If the highest rate at which frames are not lost is equal to or exceeds the threshold, the test indicates that the test passed for each transmitted frame length. If it falls below the threshold, the test indicates that the test failed.

Latency (RTD) test

If the Latency test is a desired part of the test, the Throughput test must also be run.

About the latency test

The Latency test transmits traffic at a specified percentage of the bandwidth at which no frames were lost (as determined during the Throughput test) for each frame length you selected. The average delay is then measured after transmitting traffic for each frame length for the period of time that you specified as the Latency (RTD) Trial Duration.The test measures delay for each trial (specified as the Number of Latency (RTD) Trials), and each measurement is then added to a running total. After all of the trials are complete, the running total is divided by the number of trials to come up with a total trial average.

If the Throughput test reached the lowest bandwidth limit without ever successfully receiving all transmitted frames (in other words, it lost frames), the average delay will also be unavailable. Delay measured under 4 microseconds is averaged as 4 microseconds. Unavailable measurements are not included in the total trial average.



NOTE:

When running the Latency test in asymmetric mode, after looping up the instrument on the far end, the instrument performs a *symmetric* throughput test. Because the instrument loops up the far end instrument, the upstream and downstream latency measurements in asymmetric mode are actually the same measurement. All other tests are performed end-to-end (no loopback is performed).

Pass/fail threshold

You can configure the test to optionally indicate whether the Latency test passed or failed. To do so, you specify the Latency (RTD) Pass Threshold. If the total trial average for measured average delay is equal to or less than the threshold, the test indicates that the test passed for each transmitted frame length. If it exceeds the threshold, the test indicates that the test failed.

Packet Jitter test

If you intend to run the Packet Jitter test as part of the test, you must also run the Throughput test.

About the Packet Jitter test

The Packet Jitter test transmits traffic at the maximum bandwidth at which no frames were lost (determined using the Throughput test) for each frame length you selected. The packet jitter is then measured after transmitting traffic for each frame length for the period of time that you specified as the Packet Jitter Trial Duration.

The test measures the average packet jitter and maximum packet jitter for each trial (specified as the Number of Packet Jitter Trials), and then each measurement is added to a running total. After all of the trials are complete, the running total is divided by the number of trials to come up with a total trial average measurement.

If the Throughput test reached the lowest bandwidth limit without ever successfully receiving all transmitted frames (in otherworlds, it lost frames), the packet jitter measurements will also be unavailable. Unavailable average or maximum average measurements are not included in the total trial average.

Packet Jitter test results

Packet Jitter results are presented statistically.

Pass/fail threshold

You can configure the test to optionally indicate whether the Packet Jitter test passed or failed. To do so, you specify the Packet Jitter Pass Threshold. For each frame length you selected, the test compares the average packet jitter for the trial to the value that you specified as the threshold. If the average packet jitter is less than or equal to that specified for the threshold, the test indicates that the test passed. If it exceeds the threshold, the test indicates that the test failed.

About the System Recovery test

If you intend to run the System Recovery test, the Enhanced RFC 2544 mode must be Symmetric, and you must also select and run the Throughput test.

About the System Recovery test

The instrument uses the Throughput test to determine the maximum bandwidth at which no frames were lost, then the System Recovery test transmits traffic at 110% of the bandwidth (referred to as the “overload rate”) to force the receiving network element to drop frames for each frame length you selected. The instrument transmits the overload rate for at least 60 seconds, then reduces the trans-

mission rate to 50 percent of the overload rate (referred to as the “recovery rate”). The instrument then measures the time it takes for the network element to reach a state where it is no longer dropping frames.

If the Throughput test reaches the lowest bandwidth limit without ever successfully receiving all transmitted frames (in otherworlds, it lost frames), the System Recovery test will not run.

For optimum results, the system recovery test should be run for at least 30 seconds.

System Recovery test results

System Recovery results are presented statistically and graphically.

Frame Loss test

The Frame Lost test measures bandwidth until no frames are lost.

About the frame loss test

For each frame length you select, beginning at the maximum test bandwidth you specified, the instrument transmits traffic for the amount of time you specified as the Frame Loss Trial Duration. If frames are lost during that time frame, the instrument reduces the transmitted bandwidth by the amount you specified as the Frame Loss Bandwidth Granularity, and then transmits the traffic at the reduced bandwidth.

The test decreases the transmitted bandwidth accordingly until either no frames are lost during the duration specified, or the transmitted bandwidth reaches the lowest bandwidth limit (specified as the Frame Loss Bandwidth Granularity).

If the instrument succeeds in transmitting frames without losing any at a particular bandwidth, it then reduces the bandwidth one more time (by the granularity amount). If no frames are lost, the test stops. If frames are lost, the instrument starts the entire process over again until two successive trials occur without losing frames.

Frame Loss test results

Frame Loss results are presented in a tabular format, illustrating the frame loss rate versus the percent of the bandwidth.

Back to Back Frames test (Burst test)

This test determines the maximum back to back burst size supported by the network under test.

About the Back to Back Frames test

Using the frame length and other settings such as the frame type and encapsulation, the instrument calculates the burst size required to transmit back to back frames for the duration that you specify as the Back to Back Max Trial Time. It then transmits the burst of frames over the circuit. If the number of frames transmitted carrying an Acterna payload does not equal the number of received frames carrying an Acterna payload (indicating that frames were lost during the transmission), the instrument goes through the stages described for the Throughput test (see “Throughput test” on page 285) until no frames are lost, or until the number of frames per burst from the last successful

burst exceeds the Back to Back Frames Granularity by a 1 frame burst.

The test counts the number of frames received for each trial (specified as the Number of Back to Back Frame Trials), and each count is added to a running total. After all of the trials are complete, the running total is divided by the number of trials to come up with a total trial average count. The test then uses this count to calculate the average amount of time a burst can be transmitted before a frame is dropped.

Back to Back test results

Back to Back test results are presented in a table.

Optimizing the test time

When you configure an Enhanced RFC test in symmetric mode, you can optimize the time it takes to run the test time by doing the following:

– Ensure that the duration time for the Throughput, Packet Jitter, and Latency (RTD) tests is the same.
– Ensure that the number of trials for the Latency (RTD) and Packet Jitter tests is “1” (one trial only).

If you configure the test in this manner, all three tests (Throughput, Latency, and Packet Jitter) will be run simultaneously. If the duration times vary, or if you indicate that you want to run more than one trial, each test will be executed in succession. As a result, the test will take longer to complete.

When running the Enhanced RFC 2544 test in asymmetric mode, the Latency test is run *after* the Throughput test, because it needs the symmetric Throughput measurement before it can measure latency.

In addition to the duration time and number of trial settings, you can control the bandwidth transmitted during the course of the test.

– If you select Top Down, the test transmits traffic at the maximum bandwidth specified, and then *decreases* the bandwidth for each trial by the granularity you specify until you reach the minimum bandwidth specified.
– If you select Bottom Up, the test transmits traffic at the minimum bandwidth specified, and then *increases* the bandwidth for each trial by the granularity you specify until you reach the maximum bandwidth specified.

Importing and exporting RFC config files

The instrument allows importing and exporting of configuration files. This allows consistent testing configurations which yield more reliable test results. You will need a USB stick for transferring the files.

To export a RFC configuration

Step1 Verify that you have a USB stick inserted into the instrument.

Step2 After specifying the settings for your Enhanced RFC test, save the configuration.

Step3 Exit the test.

Step4 From the Tools menu, select **Export to USB**, and then **Saved Test Config**.

Step5 Locate the `*.expert_rfc` file or files you wish to export. Click on the file to select it (click again to un-select it).

Step6 Do one of the following:

– If exporting multiple files and you wish to zip them before exporting, click the **Zip selected files as** box and specify a file name for the resulting .tar file, and then click **Zip &Export**.

– If exporting files without zipping or are exporting a single file, Click **Export**.

The files are copied to the USB stick.

To import a RFC configuration

Step1 Verify that you have a USB stick inserted into the instrument.

Step2 From the Tools menu, select **Import from USB**, and then **Saved Test Config**.

Step3 Locate the file or files you wish to import. Click on the file to select it (click again to un-select it).

Step4 Do one of the following:

– If importing a zipped file, click **Unzip& Import**.

– If importing one or more files that are not compressed, click **Import Test**.

The files are copied to the instrument's file directory. The next time you launch the test, the imported configuration(s) appear in the configuration list.

Initiating the Enhanced RFC2544 Test

There are two ways to initiate the RFC2544 test using the on screen softkey.

– Select the base application and then initiate the RFC2544 test using the on screen soft key.

– Select the RFC2544 implementation for the technology and interface you want to use.

The first option will be necessary if you have "No Configurations" saved where you can load the parameters of the test to be run. Alternatively, if you are coming back to run of a saved configuration (or modify an existing profile), you can select the direct initiation of the automatic script, load the existing profile and start testing. For more information see "Launching a single automated test" on page 279.

Configuring the Enhanced RFC 2544 or Fibre Channel tests

Before running these tests, it's important to understand which settings need to be specified externally (outside of the automated test screens), and how to navigate through the screens and menus presented when you run the tests.

Specifying the external test settings

The automated tests allow you to specify most required settings; however, certain settings need to be specified outside of the automated test screens (using the procedures listed in Table 29.

Table 29 RFC 2544 and Fibre Channel Setup Tab Settings

Layer/Setting	To specify, see....
Ethernet Layer 2 – Frame Type – Destination Type – Ether Type – Unit Identifier	"Specifying Ethernet frame settings" on page 49 "Specifying interface settings" on page 46
Fibre Channel Layer 2 – Flow Control: ON	"Specifying interface settings" on page 252
Layer 3 – ARP – TTL – TOS/DSCP	 "Specifying Ethernet frame settings" on page 49 "Specifying transmitted IPv4 packet settings" on page 83
Layer 4 – ATP Listen Port	"Specifying TCP/UDP settings for transmitted traffic" on page 153

To specify the external test settings

Step1 Select the **Setup** soft key, and then do one of the following:

– If you are running the test with layer 2 Ethernet traffic, select the Ethernet tab to specify settings that define the frame characteristics of the transmitted traffic, such as an 802.3 frame type, or a VLAN ID and priority (see "Specifying Ethernet frame settings" on page 49).

– If you are running the test with layer 3 Ethernet (IP) traffic, select the Ethernet tab to enable or disable ARP, and then select the IP tab to specify settings that define the packet characteristics of the transmitted traffic, such as the destination IP address (see "Specifying transmitted IPv4 packet settings" on page 83).



NOTE:

If running two 6000/8000 instruments end-to-end, keep in mind that the instrument's PPPoE server is a demo server and does not support full server functionality. Thus, round trip delay cannot be measured. To measure round trip delay, use a network server.

– If you are running the test with layer 2 Fibre Channel traffic, select the Fibre Channel tab to specify settings that define the frame characteristics of the traffic (see "Specifying Fibre Channel frame settings" on page 254).

– If you are running the test with layer 4 traffic, select the TCP/UDP tab to specify the listen port settings and indicate whether you want to transmit TCP or UDP traffic (see "Specifying TCP/UDP settings for transmitted traffic" on page 153).

Step2 Verify the following settings:

– Payload analysis is ON for your current test application. You can not run the RFC 2544 or Fibre Channel test when the module is configured to analyze live traffic.

– Traffic is not VPLS or MPLS encapsulated. You can not run the RFC 2544 test with VPLS or MPLS encapsulated traffic.

– The module is not configured to run a timed test. You can not run the RFC 2544 or Fibre Channel test during a timed test.

Step3 Select the **Results** soft key to return to the Main screen.

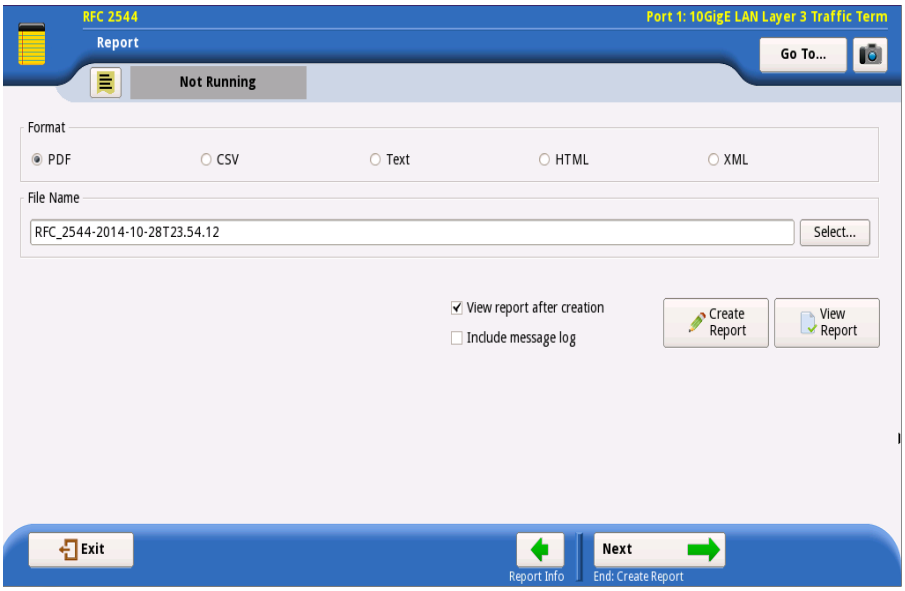
The external settings are specified.

Setting Connection parameters

Before running any of the RFC2544 automated tests, the connection parameters must be defined so the local and remote units can link.

Configuration methods

Upon initiation of the RFC2544 Automated configuration, the user is given the option of defining all parameters manually or restoring a configuration from a previously saved file. In either case any parameter may be modified prior to running the tests.



Retrieving configuration from previously saved file

Step1 To select a configuration currently saved on the unit, select the **Go** button (right green arrow) after “Load Configuration from Profile”. The interface shown in Figure 88 will appear..

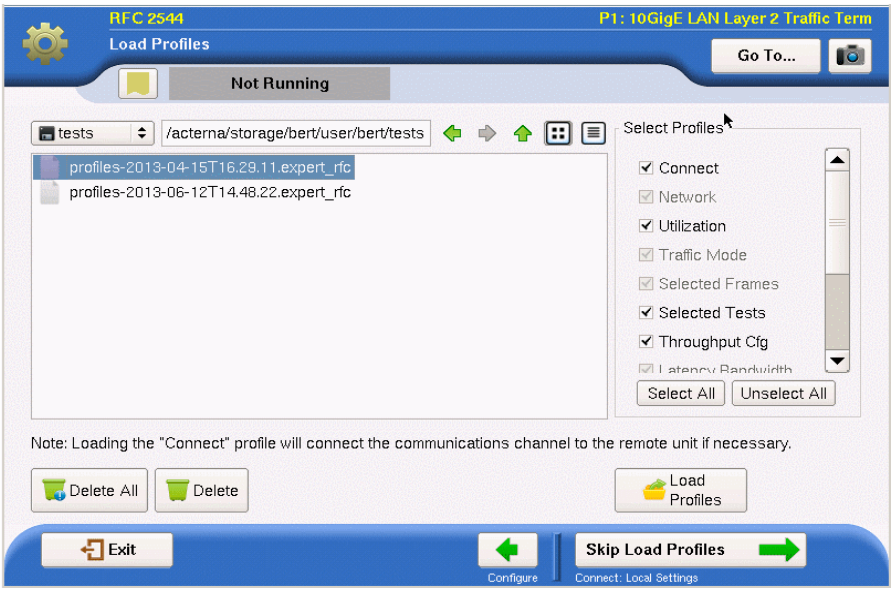


Figure 88 RFC 2544 Load Profiles screen

Step2 After selecting one of the files on the left side, the configured scripts that comprise the profile will be shown checked. To prevent any portion of the saved configuration from loading, un-check any of the activated sections. Any portion of the test may be configured after the saved file is loaded.

Step3 Select the **Load Profile** button. The test will be configured as saved and if the connect data is detailed in the file, the unit will attempt to establish that connection.

Step4 If a desired configuration is not found, select the **Skip Load Profiles** button (right green arrow). Go to step 2 of “Manually configuring all parameters” on page 294.

Manually configuring all parameters

Step1 To manually configure the tests to be run, from the main menu, select the **Go** button (right green arrow) after Configure Test Settings Manually.

Step2 The first Connection parameters screen describes the Symmetry of the connection to be established.

a Select the Throughput.

Symmetric - same parameters for up and downstream connections

Asymmetric - different up and downstream parameters

Unidirectional - only testing one direction, up or downstream

a Depending on the symmetry selected, define the Measurement Direction.

Looped

Upstream

Downstream

Select **Next** (the green arrow).

Step3 For all symmetry schema, except loop back, the Connection parameters pertaining to the local and remote instrument must be defined.

a The first screen specifies the local settings. These parameters are Frame Type, and IP Settings - Source IP, Gateway and Subnet Mask.

Other optional settings are accessed via the **Advanced** button they are

MAC Address Source and Number, ARP Mode and Source IP type.

When all local settings have been specified, select **Next** (the green arrow).

b The Remote configuration screen defines the number of VLANs and the Destination IP.

– To verify the Destination instrument is available, select the **Ping** button.

– To establish the connection with the remote instrument, select the **Connect to Remote** button.

If the test is being configured for future use and/or the remote instrument is not available, to continue with the configuration, select the **Skip Connect** right arrow button.

Step4 The next set of parameters to be defined pertain to network configuration. Depending upon the symmetry scheme selected, screens defining the following will appear in sequence.

Unit	Parameter	Options
Layer 2	Frame Type	DIX 802.3
	Encapsulation	NONE VLAN Q-in-Q Stacked VLAN
	Source IP	User entry
	Default Gateway	User entry
	Subnet Mask	User entry
	Advanced	Source MAC ARP Mode (L3, L4) Source IP type (L3, L4)
Layer 3 (L3 & L4 applications only)	IP Prioritization	NONE TOS DSCP PPPoE
	TOS	User entry
Layer 4 applications only)	Traffic Mode	TCP UDP
	Source Service Type	Select from list
	Source Port	User entry
	Destination Service Type	Select from list
	Destination Port	User entry

Test selection

After all connection parameters have been defined, the user is able to select which tests are to be included in the automated sequence. In addition to the standard RFC 2544 tests: Throughput, Latency, Frame Loss, Back to Back and System Recovery (loop back only), additional tests are included for Packet Jitter, Burst and Extended Load (loop back only)

Choosing tests to be included

Step1 Upon opting to select which tests to run, one of the following screens appears.

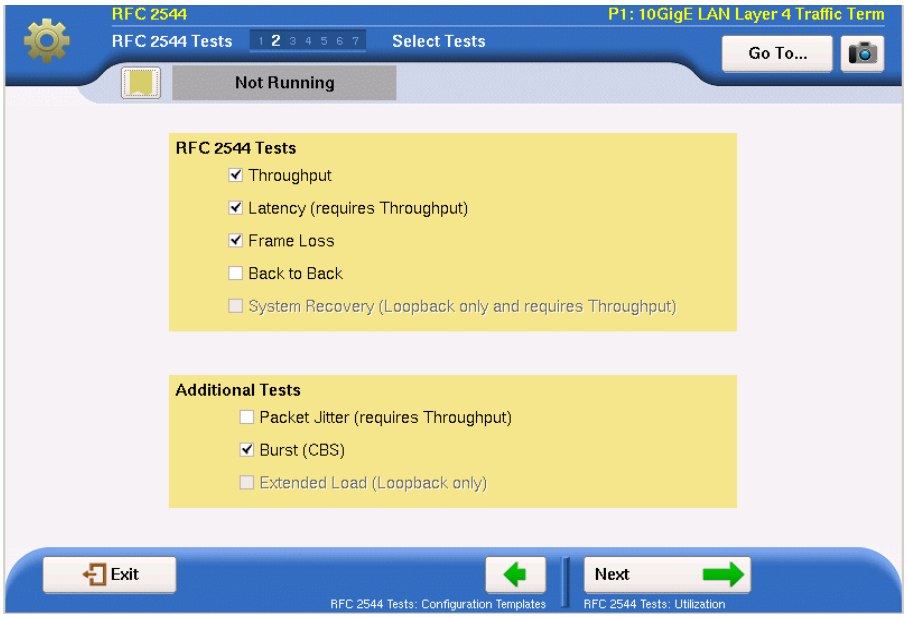


Figure 89 FC 2544 test options

The Enhanced FC tests include Throughput, Latency, Frame Loss, Back to Back, Buffer Credit and Buffer Credit Throughput.

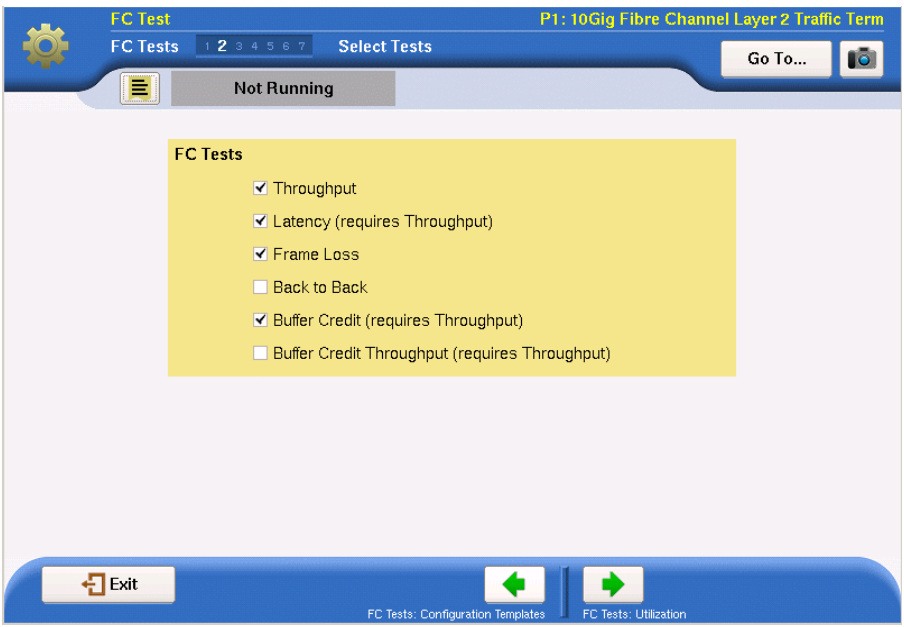


Figure 90 Enhanced FC 2544 test options

Step2 Select the tests that are to be included in the Enhanced RFC 2544 or FC automated test by checking the box in front of the tests desired. Note that some tests will be unavailable with certain connections or in combinations with other tests.

When all desired tests have been chosen, select **Next** (the green arrow).

Step3 Depending upon which test(s) have been selected there are a number of parameters that must be set to define the results.

a On the Utilization screen, the **Bandwidth Unit** and the **Max Bandwidth** can be selected.

To choose whether the bandwidth units used for the tests are chosen from **Layer 1** or **Layer 2**, make the selection in the Bandwidth Unit drop-down box. Then enter the **Max Bandwidth (in Mbps)** in the entry box (Upstream and/or Downstream for non-symmetric test).



NOTE:

The load value cannot be set to a value that cannot be measured on the other side due to an imbalanced line rate.

To further refine the Utilization configuration, select **Set advanced Utilization settings** and then select **Allow True 100% Traffic**, if desired. Select **Back** to return to previous screen.

Select **Next** (the green arrow).

b On the Frame Lengths screen, select the number of frame lengths to be tested by checking the appropriate number of boxes and then entering a value for each checked Upstream and/or Downstream Frame length to be tested.

Select **Next** (the green arrow).

c On the Throughput Test screen, select whether the RFC 2544 Standard or JDSU Enhanced version of the test is to be used for the **Zeroing-in Process** and the level of **Measurement Accuracy** (Upstream and/or Downstream for non-symmetric test).

To further refine the Zeroing-in Process configuration, select **Set advanced Throughput Latency measurement settings** and then specify the **Latency Bandwidth**. Select **Back** to return to previous screen.

Select **Next** (the green arrow).

d On the Frame Loss Test screen, select the test procedure to be used.

RFC 2544. Transmits traffic at the maximum bandwidth, and then decreases the bandwidth for each trial by the granularity you specify. The test ends after two successive trials with no frames lost. This procedure also requires specification of **Bandwidth Granularity** in Mbps**.**

Top Down. Transmits traffic at the maximum bandwidth specified in the **Test Range** setting, and then decreases the bandwidth for each trial by the **Number of Steps** specified until the minimum bandwidth is reached for the specified Test Range.

Bottom Up. Transmits traffic at the minimum bandwidth specified in the **Test Range** setting, and then increases the bandwidth for each trial by the **Number of Steps** specified until the maximum bandwidth is reached for the specified Test Range.

To further refine the frame loss configuration, select **Set advanced Frame Loss measurement settings** and then choose whether to **Measure Latency** or **Measure Packet Jitter** by selecting their checkbox. Select **Back** to return to previous screen.

Select **Next** (the green arrow).

e For the Back to Back Test screen, define the **Max Duration** (Upstream and/or Downstream for non-symmetric test) of each test and **Burst Granularity** in kB.

To further refine the Back to Back test, select **Set advanced Back to Back settings** and then choose the **Ignore Pause Frames** checkbox. Select **Back** to return to previous screen.

f For the Burst Test screen, select the Burst Test Type - either **Committed Burst Size**, **CBS Policing (MEF 34)** or **Burst Hunt** and the **CBS (in kB)** (Upstream and/or Downstream for non-symmetric test), **CBS Duration** and **Burst Sizes (kB**) (Upstream and/or Downstream for non-symmetric test) depending on which Burst test type is chosen.

g For the Extended Load test screen, enter **Throughput Scaling (%)** and **Frame Length** values.

Select **Next** (the green arrow).**Next** (the green arrow).

h For the Buffer Credit screen (FC only), enter the Flow Control Login Type - **Implicit** or **Explicit**; the **Max Buffer Size** and the **Duration** of each test in seconds.

When the individual tests have been configured, select **Next** (the green arrow).

Step4 The overall test control configuration items need to be set.

a On the Test Duration screen, specify whether all tests are to have common durations or are individual tests to have their durations specified separately by selecting **Yes** or **No** radio button.

If Yes is chosen specify the **Durations** and the **Number of Trials**.

Select **Next** (the green arrow).

b On the Test Thresholds screen, specify whether **Pass/Fail** indications are to be shown for individual tests and what is the pass/fail **Threshold** value (Upstream and/or Downstream for non-symmetric test) for each test.

When the overall test control configuration items have been set, select **Next** (the green arrow).

Step5 The RFC 2544 test has been completely configured.

a If it is not desired to save this configuration profile, at this time, go to step 6.

b To save the profile of this configuration, specify the filename under which it is to be saved by entering the desired filename in the **File Name** box. To discover the name of previously saved files click on **Select**.

To preserve the configuration so it won't be changed by future users, select the **Save as read-only** checkbox.

When all file attributes have been set, select the **Save Profiles** button. and then select **OK** to return to the previous screen.

Select **Next** (the green arrow).

Step6 The Run/Edit screen appears.

Do one of the following:

– To return to the beginning and modify the current configuration, select the **Go** arrow after "Change Configuration". Go to "Manually configuring all parameters" on page 294.

– To load a previously saved set of configuration parameters, select the **Go** arrow after "Load Configuration from a Profile". Go to "Retrieving configuration from previously saved file" on page 294.

– To run the test, as configured, select the **Go** arrow after "Run Tests". The Run J-Quick-Check screen appears. Go to "Running Enhanced RFC 2544 and FC tests" on page 298

Running Enhanced RFC 2544 and FC tests

After configuration has been completed, the Enhanced RFC 2544 or FC tests can be run.

The first test to be run is the J-QuickCheck test. The J-QuickCheck application uses the configured parameters for the connection to either run a bi-directional test or establish a loop back to verify that the link can support 100% traffic utilization allowing the other tests to be run effectively.

The balance of the tests will run without any user intervention necessary after initiation.

Initiating J-QuickCheck test

Step1 The screen in Figure 91 appears. Notes appear on the left side of the screen indicating the current settings to be used for the test. If different settings are desired for throughput and Frame parameters, click the **Not what you wanted?** link.

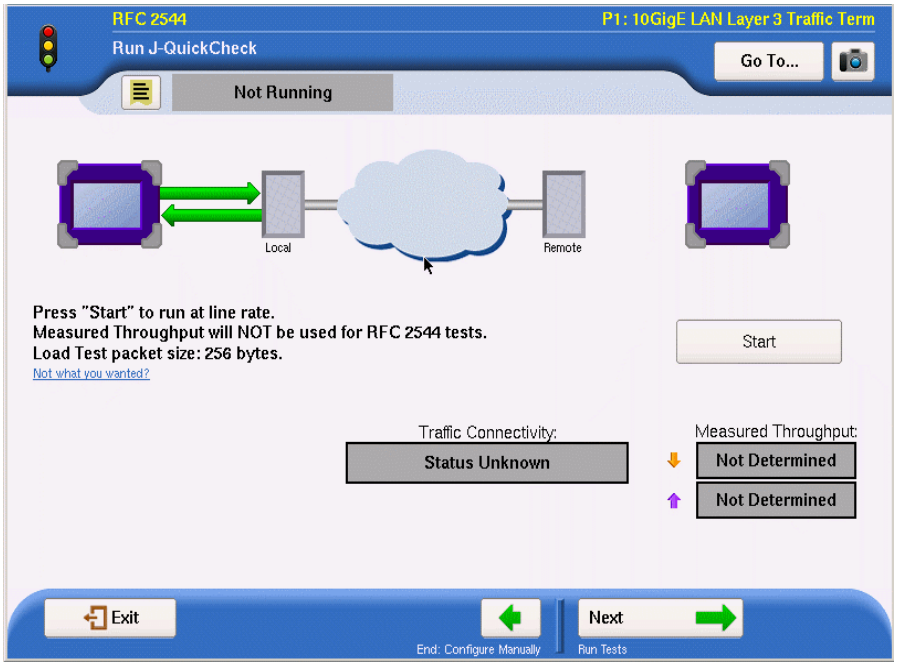


Figure 91 J-QuickCheck Screen

a Select the **Test using configured RFC 2544 Max Bandwidth** or **Use the Measured Throughput measurement as the RFC2544 MAx Bandwidth** check boxes and/ or enter a new frame size value via the pop-up keypad.

b Select **Back** to return to previous screen.

Step2 To initiate the J-QuickCheck test, press the **Start** button.

Step3 Observe the network diagram. The following occurs:

a For both end running terminate application - The instrument indicates that it is waiting for a link, then connecting the link, and provides the status of the auto-negotiation capabilities. If negotiation succeeds, the Traffic Connectivity box will turn green and display PASS.

b For remote loop back -The instrument sends a loop down, followed by a loop up. If the second attempt fails:

– If running a Layer 2 test:

The instrument checks for a hardware loop. If a hardware loop is not found, we check for a permanent loop. If a permanent loop is not found, the instrument declares “No Loop Found”.

– If running a Layer 3 or 4 test:

The instrument checks for a permanent loop. If a permanent loop is not found and if ARP is Disabled, the instrument checks for a hardware loop. If a hardware loop is not found, the instrument declares “No Loop Found”. If ARP is Enabled, the instrument declares “No Loop Found”.

– The instrument checks for an active loop. If there is none, it issues a loopup command to establish the loop. If the command fails, it sends it a second time. If the second attempt fails, the instrument checks for a hard loop on the far end. If a hard loop is not found, the instrument checks for a permanent loop. Finally, the status of the remote loop up appears.

Step4 If the loopup is successful (indicated with a green arrows to and from the remote unit or green loop arrow at remote), the instrument moves on to transmit traffic over the link at 100% of the line rate to verify the link’s ability to support a full load of traffic. If the test is successful, the button under Measured Throughput displays the expected throughput (Up and Down if appropriate).

Green graphics on the screen indicate that an action was successful, yellow indicates an action is currently taking place (for example, connecting the local port to the link), and red indicates that an action failed (for example, the remote loop failed).

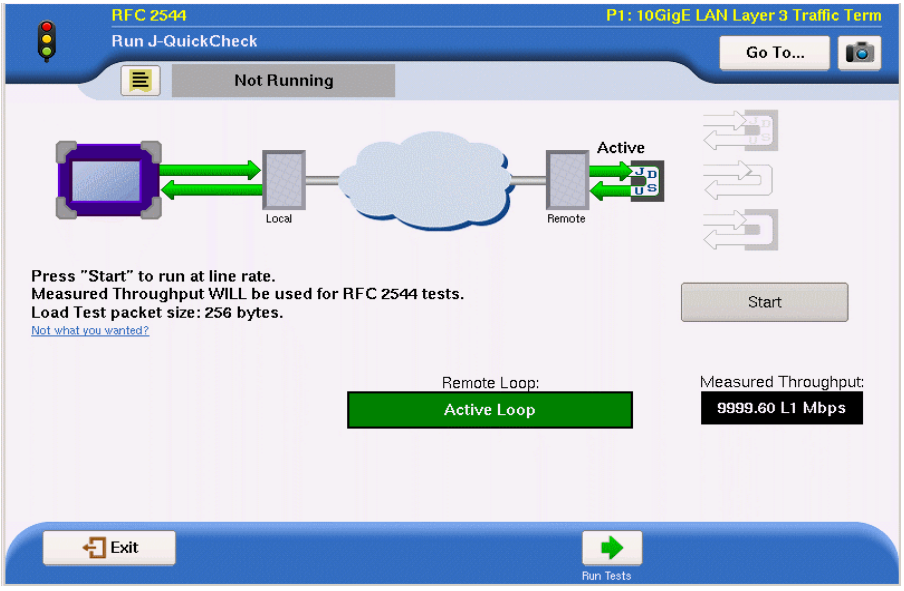


Figure 92 J-Quick Check Complete

When J-QuickCheck has reported acceptable results, select **Next** (the green arrow).

Initiating Enhanced RFC 2544 or FC test

The RFC 2544 testing status screen keeps the user informed of the progress and the success or failure of the tests while they are running. A key of status indicators is available on the screen for easy reference.

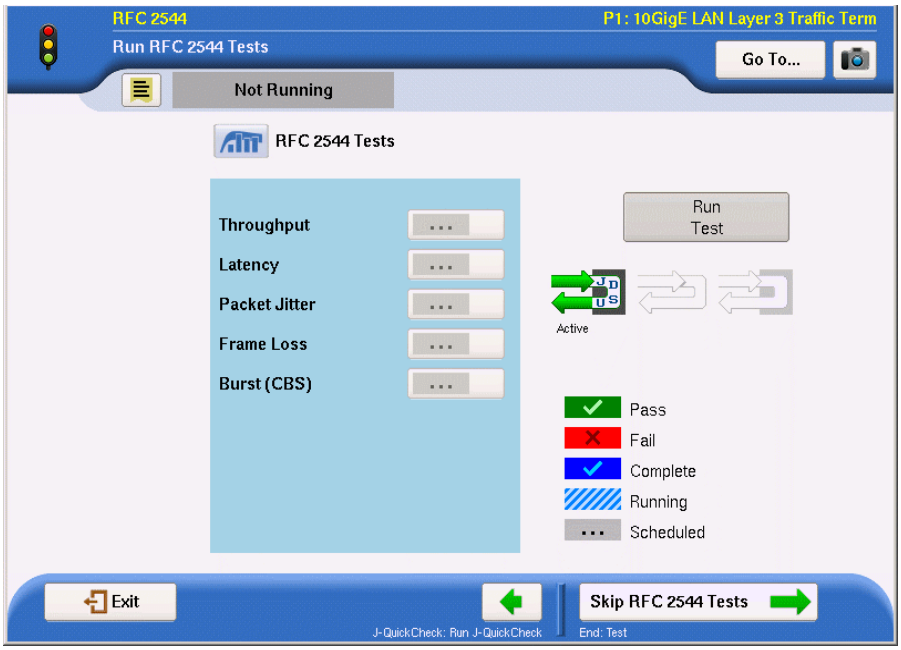


Figure 93 RFC Run Tests status screen

Step1 To initiate the test sequence, select the **Run Test** button.

The time remaining displays in the top tab, and each test scheduled will be displayed with its current status.

NOTE:

To switch between the test and the Setup panel on the user interface, click the **Go To** button at the top of the screen and then click the **Results** button in the dialog. This function is intended allow you to verify the settings. Note that the RFC2544 button is yellow to indicate it has been launched. You should not change the settings during a test, as you may get undesired results. To return to the test, click the RFC2544 button.

Step2 When the tests have completed, select the **Next** (the green arrow).

The Test Complete page appears.

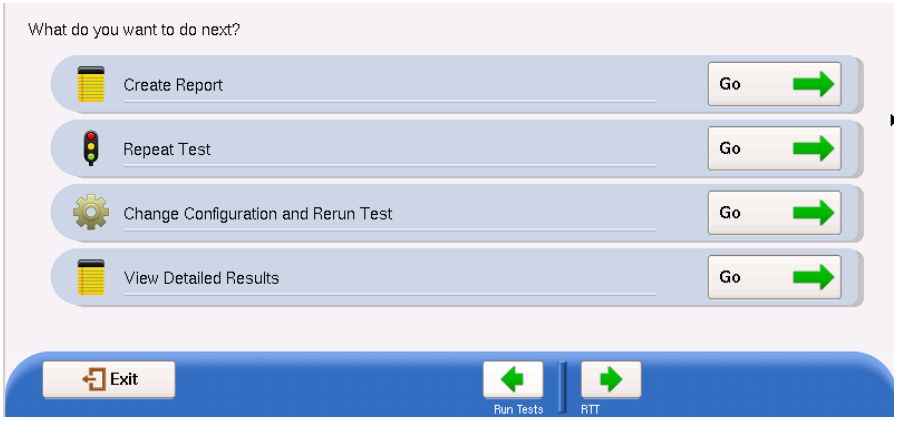


Figure 94 Enhanced RFC 2544 or FC Post-test Window

Do one of the following:

– To create a report of the results of the test that just completed, select the **Go** arrow on the "Create Report" line. Go to step 3.

– To repeat the test that just ran, select the **Go** arrow on the "Repeat Test" line. Go back to "Running Enhanced RFC 2544 and FC tests" on page 298.

– To reconfigure the test and then run it again, select the **Go** arrow on the "Change Configuration and Rerun Test" line. Go to step 2 of "Manually configuring all parameters" on page 294.

– To view detailed results of the performance achieved during the test, select the **Go** arrow on the "View Detailed Results" line.

  The detailed results are presented on a sequence of windows that vary depending upon the steps in the test that were selected to be run.

  On the last page of the results select the right-pointing green arrow. Go to step 3.

Step3 The report info screen will display.

This screen allows the user to enter information about the test environment which will be added to the report.

This information includes-

Customer Name

Technician ID

Test Location

Work Order

Comments/Notes

Custom Logo (from memory)

Step4 After all the desired data is entered into the entry boxes, select **Next** (the green arrow).

Step5 The Report window appears.

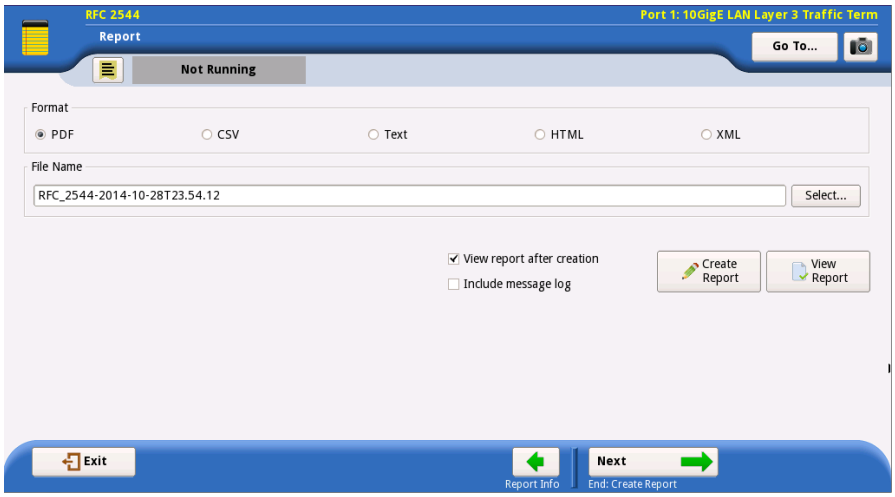


Figure 95 RFC 2544 Report Window

Do the following:

a Select the format in which the report is to be saved by selecting the radio button in Format pane.

b Specify the filename of the report.To review the filenames of other, currently saved reports on the unit, select the Select button.

c You may view saved reports by selecting the **View Report** button.

d To show a copy of the current report after saving it, check the **View report after creation** checkbox. The report will automatically load into the appropriate reader (if available) depending upon the format in which it has been saved.

e To include the message log with the report, select the Include Message log check box.

f When ready to save the report, select the **Create Report** button. After it has been saved (and viewed), select the right-pointing green arrow.

Step6 The post-report/results window appears.

All options available on this window are described in step 2 with the exception of the “Exit RFC 2544 test”.

To exit the RFC 2544 test application, select the **Go** arrow after “Exit RFC 2544 test”.

Step7 The Exit window appears.

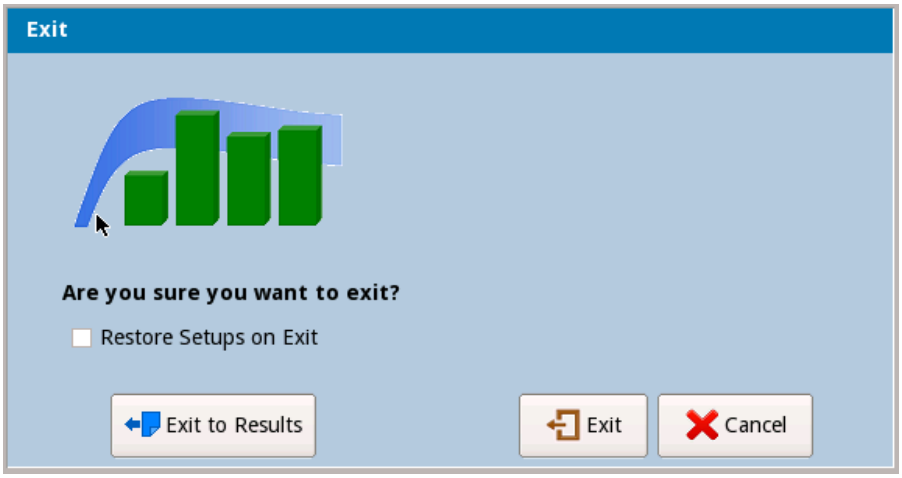


Figure 96 Enhanced RFC 2544 or FC test exit page

Do one of the following:

– To exit to the base application, retaining all setups from the RFC2544 test, select the Exit to Results button.

– To restore the configuration setups to their default values when leaving the application, check the box **Restore Setups on Exit**. To completely exit the Enhanced RFC 2544 or FC application, select **Exit.**

– To return to the previous window, select **Cancel**.

The Enhanced RFC 2544 or FC test has been run.

SAMComplete

This test is a multi-stream test based on ITU-T Y.1564 that performs a two-phase test. First, the test verifies whether each Ethernet service is properly configured. Second, multiple Ethernet service instances are verified simultaneously, each meeting its assigned Committed Information Rate (CIR). All services are transmitted at CIR and must pass all SLA parameters (FDV, FTD, RTD and Availability).

The following topics are discussed in this section:

– “Initiating the SAMComplete test” on page 305
– “Configuring SAMComplete test settings” on page 306
– “Choosing SAMComplete tests” on page 314
– “Running SAMComplete tests” on page 314

Initiating the SAMComplete test

SAMComplete functionality is standard on all units and all Ethernet line rates are supported. Although all applications do not include SAMComplete functionality, if your instrument is appropriately configured for a capable application (such as Traffic Terminate or Multistream application on Layer 2 or Layer 3; or the TCP Wirespeed application on Layer 4), you can use it to run the SAMComplete test.

There are two ways to initiate the SAMComplete test; both from the Select Test application tree.

– Select the base application and then initiate the SAMComplete test using the on-screen softkey.
– Select the SAMComplete implementation for the technology and interface you want to use.

The first option will be necessary if you have no configurations saved to load the parameters of the test to be run. Alternatively, if you are coming back to run a saved configuration (or modify an existing profile) you can select the direct initiation of SAM Complete, load the existing profile and start testing. For more information see “Launching a single automated test” on page 279.

To launch the SAMComplete test (from base application)

Step1 If you haven’t already done so, use the Test Menu to select the desired application for the circuit you are testing (see “Launching a single automated test” on page 279), and connect the instrument to the circuit. For details, refer to the *Getting Started Manual* that shipped with your instrument or upgrade.

Step2 Select theSAMComplete soft key on the right side of the interface.

If the soft-key is grayed out, the test cannot be launched. This is typically due to an invalid setup setting. For example, you are configured for VPLS/MPLS, Stacked VLAN, or PPPoE.

Step3 Go to “Configuring SAMComplete test settings” on page 306

SAMComplete has been launched.

To Launch SAMComplete simultaneously with base application

Step1 From the Select Test application tree, select the technology and interface desired. All the applications available for the current configuration of the unit will be displayed.

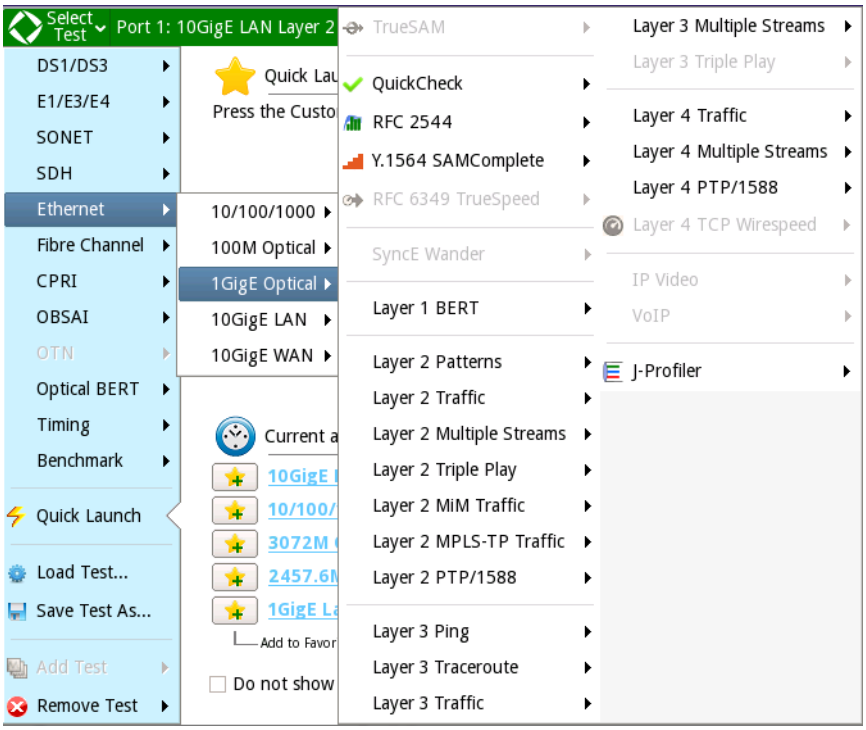


Figure 97 Test Select Tree

Step2 Select Y.1564 SAMComplete from the tree, then the specific test desired such as Layer 2 Traffic >Term.

Step3 Go to "Configuring SAMComplete test settings" on page 306.

SAMComplete has been launched.

NOTE

The Quick Launch window displays previously run and/or saved configurations of applications. Automated scripts launched simultaneously with base applications are fully identified with the script and base application. See *T-BERD/MTS 8000, 6000A, and 5800 Multiple Services Application Module, 40/100G Transport Module, 100G Services Application Module, Dual Module Carrier, and Handheld Network Test Family Getting Started Manual* for more information on the Quick Launch window.

Configuring SAMComplete test settings

From the configuration page, the settings can be configured manually, or if a profile has been previously configured and saved, the test settings can be loaded into SAMComplete.

To configure test settings

To make changes to the existing settings, select the green arrow to the right of Edit Previous Configuration. Go to step 2 on page 307.

To reset all settings to their default values and configure all options yourself, select the green arrow to the right of **Start a New Configuration**. Go to step 2 on page 307.

To load configuration settings set from a previously saved file, select the green arrow to the right of **Load Configuration from a Profile**.

Step1 The Profile selection window appears.

The filenames of the saved profiles will be listed on the left side of the window and all sections of the currently loaded profile will be listed on the right side of the screen.

Do the following:

a Select a profile from the list whose configuration is to be loaded.



NOTE:

If you load a profile that was configured on another unit, and that profile specified including a logo in the test report, make sure that the .png, .jpg, or .jpeg is in the following folder on your unit: `/acterna/user/disk/bert/images`

b Check those sections, on the right side of the screen, that are to be loaded into the test. If no profile has yet been selected, the currently configured profile sections will be checked.

Any section not selected will not be configured into the test. Any parameter of the test (checked or not checked) may be reconfigured at a later point in the configuration process.

c Select the **Load Profiles** button to load all checked sections into the test. After profile has successfully loaded select, **OK** and then select **Next** (the green arrow). Go to "Choosing SAMComplete tests" on page 314.



TIPS:

1. Generally, selecting the **Next** button (right green arrow) on each page will advance to the next step you need to do, but if at any time, you need to return to the test configuration, skip to running tests, or review test results, select the **Go To...** button, and then select the step to which you need to return.

2. To save a view of the screen on the unit for future reference, use the camera icon to capture a screenshot.

Step2 The first Symmetry page appears.

Do the following:

a Select the Throughput type:



NOTE:

Bidirectional tests must be initiated on an MSAM. The remote unit may be an MSAM, T-BERD/MTS 5800 or a Transport Module. An HST-3000 (with Ethernet SIM) cannot be used for bidirectional tests.

Symmetric – used where only one set of throughput parameters are defined because upstream and downstream transmission is identical as the signal is being looped back to the source or transmitted both downstream and upstream simultaneously.

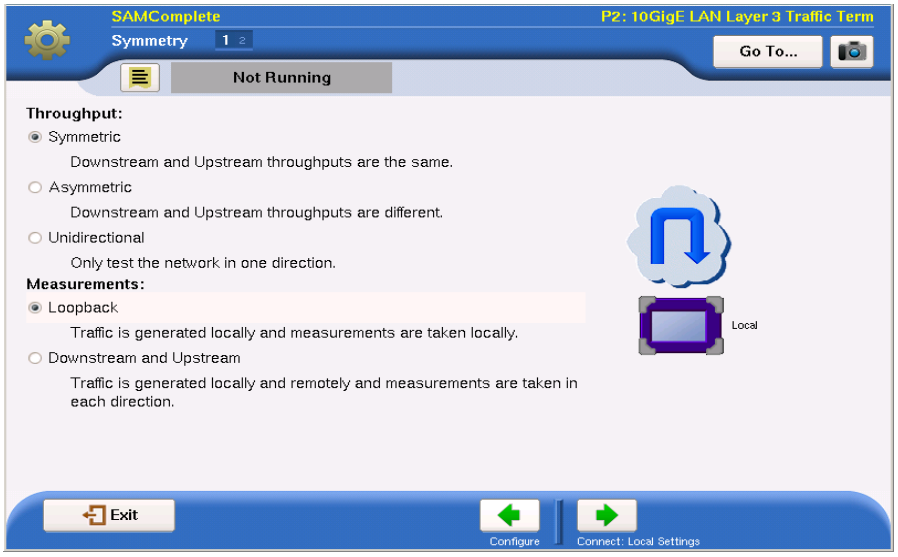


Figure 98 Symmetric Connection - Loopback Option

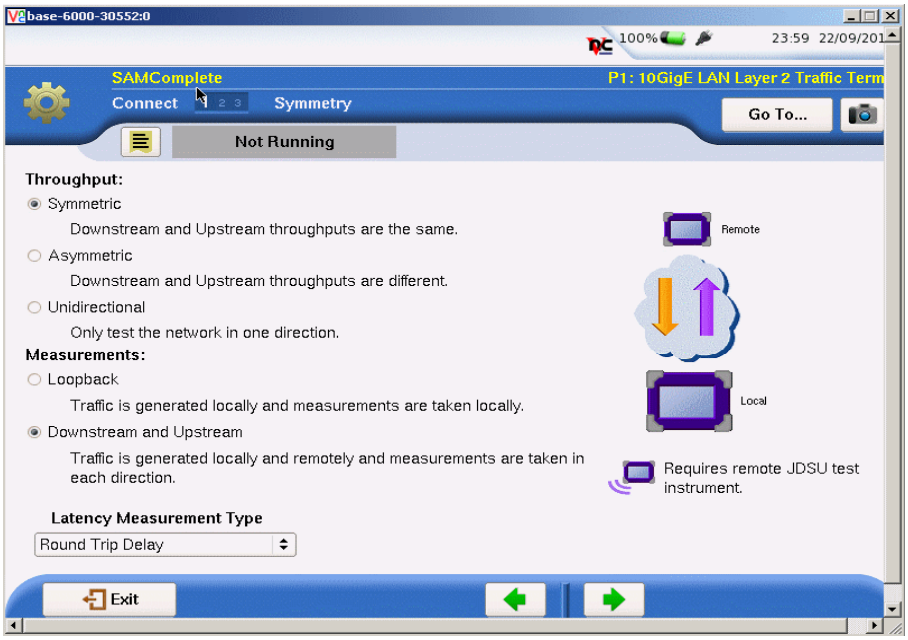


Figure 99 Symmetric Connection- Bidirectional Option

NOTE:

The Delay measurement types available when doing bidirectional testing is dependent upon the capabilities of the two units. Both units must be capable of One Way Delay to use One Way Delay and both must be capable of Bidirectional RTD to do Bidirectional RTD.

Asymmetric – used where upstream and downstream parameters in a bi-directional test are individually specified and may be different.

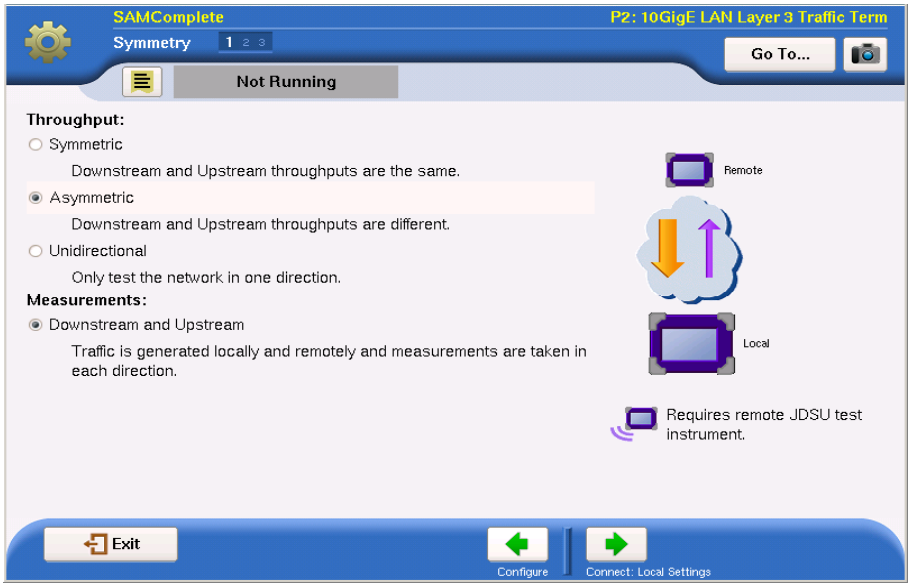


Figure 100 Asymmetric Connection Option

NOTE:

ARP must be enabled on both units if running a bi-directional SAMComplete test in L3 or Wire-speed applications.

Unidirectional – test is only conducted in one direction. May be either upstream or downstream.

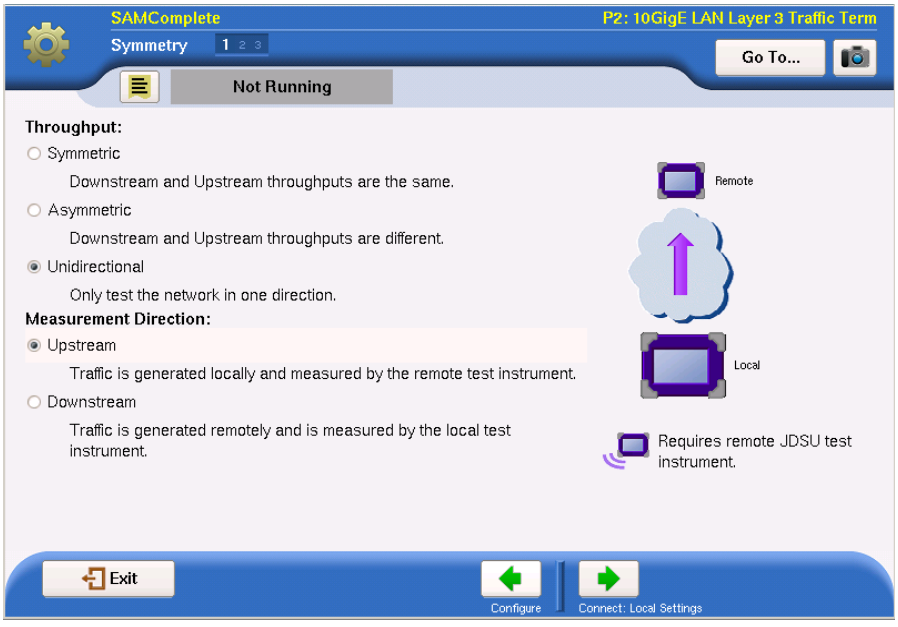


Figure 101 Unidirectional Connection Options

b Depending upon the chosen Throughput Type, select Loopback or One-Way Transmission and Direction, if needed:

– Loopback - only available with Symmetric throughput type as the signal is being looped back to the source, thus identical parameters are required.

– One-Way Transmission - tests are only conducted in a single direction. For Unidirectional Throughput type direction, Upstream or Downstream must be specified.

c If unit is configured with the One-Way Delay (OWD) sync hardware, One-Way Delay will be an option in the Latency Measurement Type selection box.Otherwise only RTD measurements will be available.

Note that the diagram on the right of the interface page indicates the type of testing to be done, and indicates if a second JDSU test instrument is required at the remote location.

d Select **Next** (the green arrow).

5 The Local Settings page appears.

Do the following:

a Specify the IP Settings (Source IP, Gateway and Subnet Mask) for Remote Connections (Channel to Far End). This is not applicable for Loopback testing so there is nothing to define.

b Advanced users: Select the **Advanced** button to specify other settings-

– Source MAC

– User Source MAC

c Select **Next** (the green arrow). For Loop back go to step 7 on page 310.



NOTE:

If you are running SAMComplete, please take note of the following facts:

The default ATP version is ATPv2.

For high-resolution between two instruments running SAMComplete, set both units to ATPv3.

Step6 The Connect to Remote page appears.

a Specify the type of tagging employed by selecting the radio button for the desired type.

b Enter the IP address of the Destination device.

c On Layer 3 or Layer 4 applications, to verify that there is a device at the address specified, select the **Ping** button. If there is a device, a green check mark will appear beside the Remote IP address.

d To connect to the remote unit, press the **Connect to Remote** button. When the Communications Channel display turns green, a valid connection to the remote device has been made.

e Select **Next** (the green arrow). If **Skip Connect**, is selected, the configuration will advance to the next step without making the connection.

Step7 The Local Network Settings page appears. Do the following:

a If a multistream application is being configured, select the number of services to be configured.

b Select the **Service Name** for each of the services being configured. This specifies which service you are configuring.

c Select configure Triple Play, if needed. The Triple Play properties screen appears. You can specify the properties for Voice, Data, HDTV and SDTV. Repeat for each of the services defined.

d Select the Layer for bit rate layer definition mode.

When L2 is selected, the max value of the Load unit will remain in terms of L1. L2 utilization is affected by frame size and therefore a value may be selected that is greater than can actually be transmitted.

e If a layer 3 application has been selected, enter Packet Length which will calculate and display the Frame Size.

f Select the Frame type desired - **DIX** or **802.3**.

g Choose, from the drop-down list, which encapsulation is desired - **None**, **VLAN**, or **Q-in-Q**.

h If a layer 2 loopback is being tested, select whether the test mode is to be **Traffic** or **LBM Traffic**.

i For Layer 2 applications, select the frame size from the values in the drop-down box.

j To specify Source and Destination MAC addresses, loop types and auto incrementing settings select the Advanced button or link at the lower right of the window.

k Select the **Next** (the green arrow).

l Depending on the application selected, a number of other Network Connection parameters will need to be defined on a number of additional pages. For more detail on these settings, see “Specifying Ethernet frame settings” on page 49.

m On the final Network Connection parameters page, select **Next** (the green arrow).

Step8 The SLA Throughput page appears.

a For applications with multiple specified services, the Total CIR and/or EIR can be aggregated and allocated to the individual services with a specified weight % per service. If this is desired, check the **Enable Aggregate Mode** checkbox. When Aggregate Mode is selected the CIR/EIR value in that line specifies the Aggregate CIR or EIR value that will be distributed to each service based on its configured Weight %.

b Specify the SLA values. Each service will have its own values. Depending upon the application selected, the SLA Threshold and Throughput can be specified for both the Local and Remote unit.

– **Weight %-** Only applies when Enable Aggregate Mode has been checked. The % of the total EIR and/or CIR to be applied to this service. All services % should add up to 100%. If they do not, a warning will appear at the top of the window informing you what the current total equals.

– **CIR** – Committed Information Rate. The threshold used to indicate the maximum sustained throughput guaranteed by the SLA. If the CIR is 0, the CIR test is skipped. When multiple services are specified and the Enable Aggregate Mode checkbox is not selected, values entered into the **All** line are copied to each service.

– **EIR** – Excess Information Rate. The threshold used to indicate the maximum sustained throughput allowed by the SLA by which a service can exceed the CIR. The throughput between CIR and EIR is not guaranteed. If the EIR is 0, the EIR test is skipped. When multiple services are specified and the Enable Aggregate Mode checkbox is not selected, values entered into the **All** line are copied to each service.

– **Policing** – Selects that policing be applied to the test. All traffic greater than CIR + EIR is removed by the policier. (If the test shows frame loss, the test passes – it indicates the policier is doing its job. If there is no frame loss even with the overage percentage, the test fails.) When multiple services are specified, selecting the Policing checkbox on the All (or Total) line, selects Policing for all services.

– **Max Load Display** - Calculated from the values of CIR and EIR and changes based upon policing selection, it is the maximum rate of traffic to be generated. (If policing is not selected, Max Load is CIR+EIR. If policing is selected, Max Load is CIR + 1.25xEIR, or when EIR is less than 20% of CIR, Max Load is 1.25xCIR + EIR).

– **M** – Tolerance, or delta, in traffic rate which is allowed to be received above CIR+EIR before declaring a policing failure. For some applications, the desired **M** value is specified on the SLA Throughput page. For Multistream or Truespeed applications, **M** will be entered on a following page labeled “SLA Policing”.

  Specify the desired value for **M**.

  c If it is desired to transmit the burst at a true 100% load, in those circuits that can handle the signal, select **Set Advanced Traffic Settings** and then check the **Allow True 100% traffic** checkbox. Select the left green arrow to return to SLA Throughput screen.

  d Select the **Next** (the green arrow).

Step9 The SLA Burst page appears.(If SLA Policing appears, see discussion of M above, in step a).

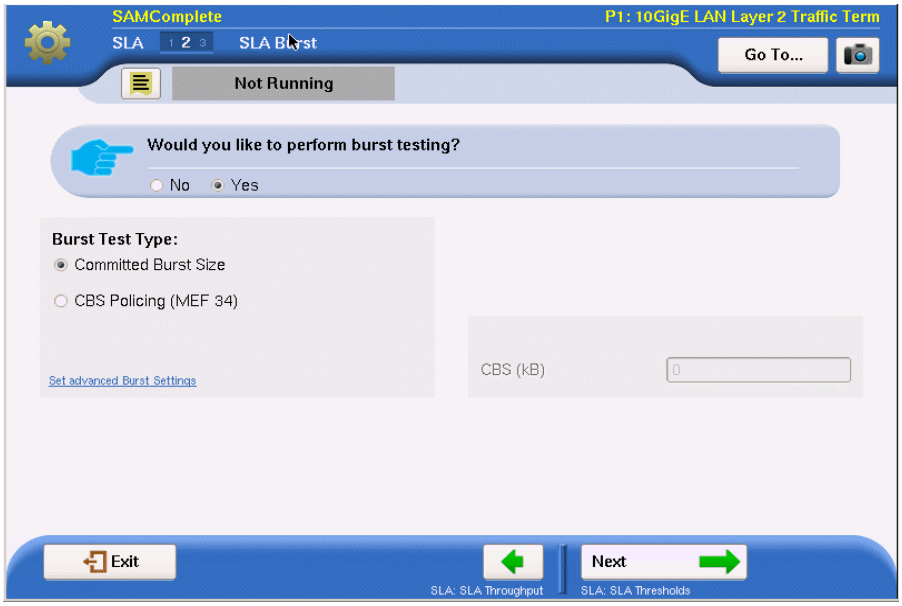


Figure 102SAMComplete SLA Burst screen

Do the following:

a Specify whether burst testing will be performed by selecting the radio button next to **Yes** or **No**.

If **No** is selected, go to step 10.

If **Yes** is selected, enter the CBS (in kB) where kB = 1000 bytes.

b Select whether to run the **Committed Burst Size** or the **CBS Policing** test by selecting the radio button next to either.

c To further refine the SLA Burst test, select the **Set Advanced Burst Setting** link.

– If desired, select the **Ignore Pause frames** checkbox.

– If CBS Policing was selected, specify the desired **+%** and **-%** tolerance to specify Pass values from expected.

– Select the **BACK** button (left green arrow) to return to the SLA Burst screen.

d Select **Next** (the green arrow).

Step10 The SLA Performance page appears.

a Specify the desired Threshold values. Each service may have its own values.

– **Frame Loss Ratio**– The maximum ratio allowed of frames lost to total frames.

– **Frame Delay** – The maximum allowed average OWD delay/latency for all throughput values.

– **Delay Variation** – The maximum allowed frame delay variation for all throughput values.

b Select **Next** (the green arrow).

Step11 The Test Controls page appears.

a Specify the Service Configuration and Service Performance settings.

– **Number of steps below CIR** – The number of steps, in information rate, needed to reach the CIR.

The corresponding number of Step Values % CIR appear. The default values will be equal parts, based on the number of steps (for example, if 3 steps are used, each will be 25%). The values can be changed, if required.

– **Step Duration** – The duration, in seconds, that traffic is generated for each step.

– **Test Duration** – The duration, in minutes, that traffic is generated before the service performance test completes.



NOTE:

When running bidirectional tests, the service performance test duration applies to each direction. So, if you run an upstream and downstream test and the test duration is set to 3 minutes, the test will run for 6 minutes.

b To further refine the Test Controls select the **Advanced** button.

% CIR – These will be automatically populated with the equal part values calculated from the Number of Steps below CIR parameter but can be changed to any value between 0 and 100.

c Select the **right green arrow**.

Step12 The Save Profiles window appears.

Do one of the following:

a If no Profile is to be saved at his time, select the **right-facing green arrow** at the bottom of the window. Go to step 13.

b If it is desired that the configuration be saved to memory (disk or USB), specify the filename. To save somewhere other than the default location, press the **Select** button after the filename to define the directory where it is to be stored.

c If it is desired that subsequent users be restricted from being able modify this profile, check the box **Save as read-only.**

d To save the file to memory, select the **Save Profiles** button. Then select the **OK** button, then select the **right-facing green arrow**.

Step13 The Run/Edit window appears.

Do one of the following:

– To return to the beginning and modify the current configuration, select the **Go** arrow after "Change Configuration". Go to step 2 of "To configure test settings" on page 306.

– To load a previously saved set of configuration parameters, select the **Go** arrow after "Load Configuration from a Profile". Go to step 1 of "To configure test settings" on page 306.

– To run the test, as configured, select the **Go** arrow after "Select and Run Tests". Go to "Choosing SAMComplete tests" on page 314

SAMComplete has been configured.

Choosing SAMComplete tests

After specifying test settings, you must choose whether to run one or both of the tests: Service Configuration or Service Performance.

To choose the tests

Step1 On the Select Y.1564 Tests page, select **Enable** if you wish to run the Service Configuration and/or Service Performance tests.

Step2 If you wish to include the optional throughput measurement in the test, check the box to enable the test, and then specify the **Max** throughput allowed.

Step3 Select **Next** (the green arrow).

The J-QuickCheck page appears. Go to "Running SAMComplete tests" on page 314.

Running SAMComplete tests

After choosing the tests, you are ready to run the test.

To run tests

Step1 From the J-QuickCheck page, do one of the following:

– Select the **Start** button.

The J-QuickCheck test, using the source and destination data entered, verifies that the connections detailed in the test setup are functioning as needed for the proper operation of the test. As J-QuickCheck is completing its analysis of the circuit, graphics along the top of the page provide a visual indication of the circuit structure and its suitability for the selected test.

If a remote device is necessary, J-QuickCheck first checks to see if a connection to the remote device has been established. If it has not, a message is displayed indicating the connection must first be established.

For Loopback tests, J-QuickCheck tests the Local port for proper operation and then checks for loopback in a remote device. If no remote active loop is detected, it then verifies whether a hard loop is in place.

After J-QuickCheck completes, select **Next** (the green arrow). Go to step 2.

– To skip the J-QuickCheck test, select the **Skip J-QuickCheck** button at the bottom of the window.

Step2 The Run Y.1564 Tests page appears.

There is a display bar for each service under Service Configuration and also for each test verdict under Service Performance. These indicate the status of each test to be run. Please refer to the Test Status Key at the bottom of the page to interpret these display bars.

Do the following:

a If you would like the test to continue when a failure occurs, un-check the **Stop on failure** box.

b Select the **Start** button.

The test begins.

As the tests are run, the status display bars will show the results of each test. In each case, you may view detailed results of that test by selecting the “magnifying glass” icon when it appears on the status bar.

While the tests are running, the status panel near the top of the screen displays a blue progress bar and indicates the estimated time remaining to complete the testing.

After the test finishes, the pass/fail results appear (green check mark or red X) on each of the tests. The status panel near the top of the screen displays an overall OK (PASS) or FAIL result

c Once the testing is completed, select **Next** (the green arrow).

NOTE:

To switch between the test and the Setup panel on the user interface, click the **Go To** button at the top of the screen and then click the **Results** button in the dialog. This function is intended allow you to verify the settings. Note that the RFC2544 button is yellow to indicate it has been launched. You should not change the settings during a test, as you may get undesired results. To return to the test, click the RFC2544 button.

Step3 The Test Complete page appears.

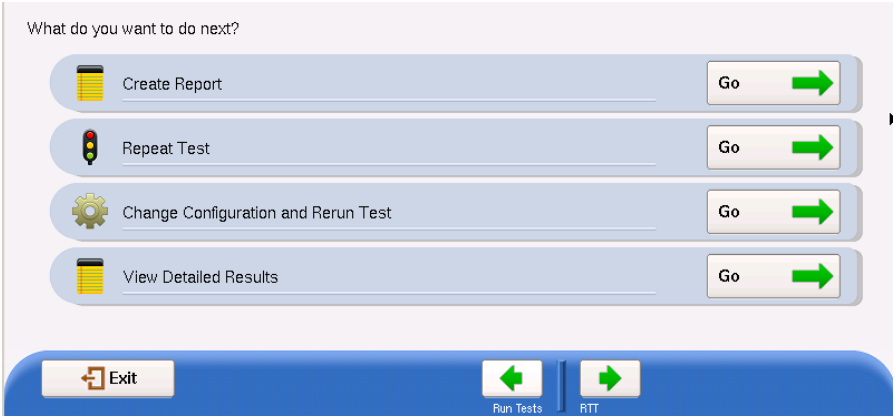


Figure 103SAMComplete Post-test Window

Do one of the following:

– To create a report of the results of the test that just completed, select the **Go** arrow on the “Create Report” line. Go to step 4.

– To repeat the test that just ran, select the **Go** arrow on the “Repeat Test” line. Go back to “Choosing SAMComplete tests” on page 314.

– To reconfigure the test and then run it again, select the **Go** arrow on the “Change Configuration and Rerun Test” line. Go to step 2 of “Configuring SAMComplete test settings” on page 306.

– To view detailed results of the performance achieved during the test, select the **Go** arrow on the “View Detailed Results” line.

The detailed results are presented on a sequence of windows that vary depending upon the steps in the test that were selected to be run.

On the last page of the results select the right-pointing green arrow. Go to step 5.

Step4 The Report window appears.

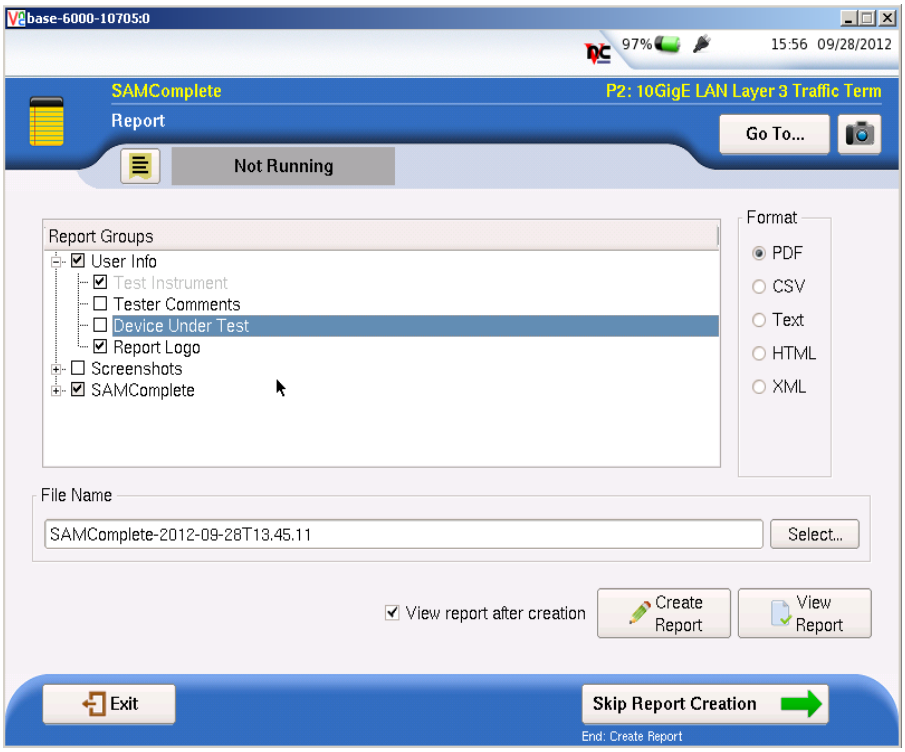


Figure 104SAMComplete Report Window

Do the following:

a Select the items to be included in the report by putting a checkmark in front of the item. Entire groups may be selected or individual items within a group. To expand the group listing to see the individual items, select the “+” in front of the group name.

b Select the format in which the report is to be saved by selecting the radio button under Format.

c Specify the filename of the report.

d You may view saved reports by selecting the **View Report** button.

e To show a copy of the current report after saving it, check the “View report after creation” checkbox. The report will automatically load into the appropriate reader (if available) depending upon the format in which it has been saved.

f When ready to save the report, select the **Create Report** button. After it has been saved (and viewed), select the right-pointing green arrow.

Step5 The post-report/results window appears.

All options available on this window are described in step 3 with the exception of the “Exit Y.1564 test”.

To exit the SAMComplete application, select the **Go** arrow after “Exit Y.1564 test”.

Step6 The Exit window appears.

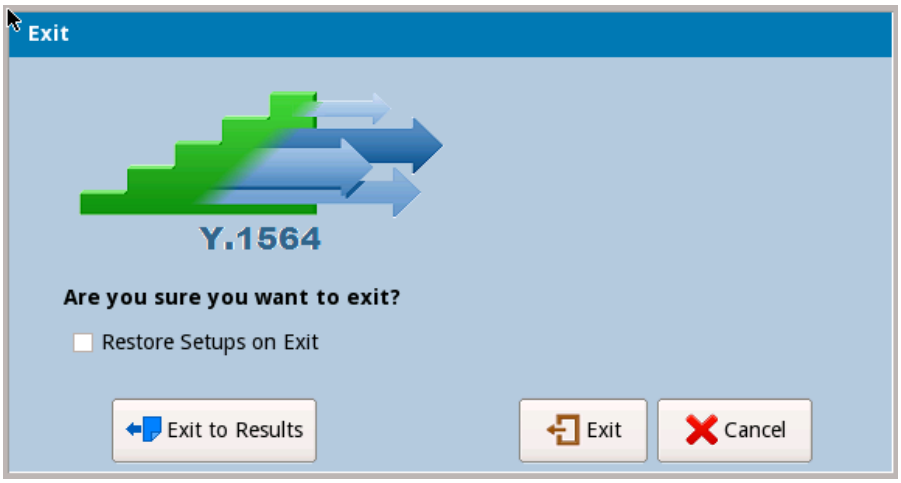


Figure 105SAMComplete Exit page

Do one of the following:

– To exit to the base application, retaining all setups from the SamComplete test, select the Exit to Results button.

– To restore the configuration setups to their default values when leaving the application, check the box **Restore Setups on Exit**. To completely exit the SAMComplete application, select **Exit.**

– To return to the previous window, select **Cancel**.

The SAMComplete test has been run.

Automated VLAN tests

If your instrument is configured and optioned to do so, you can use it to run the automated VLAN test. This test is used to test a range of VLANs by transmitting and looping back frames for each VLAN in the range for a user-specified test period, and then comparing the number of frames transmitted to the number received. Pass criteria can be specified as No frames lost or Some frames received as meet your needs.

To test a range of VLANs

Step1 Establish a LAN connection to the network using one of the Ethernet test interfaces on the Transport Module or MSAM. *Do not use the RJ-45 connector provided on the base unit*.

Step2 If you haven't already done so, use the Test Menu to select the Layer 2, Layer 3 or Layer 4 Traffic Terminate application for the circuit you are testing (see "Launching a single automated test" on page 279), and connect the instrument to the circuit. For details, refer to the *Getting Started Manual* that shipped with your instrument or upgrade.

Step3 Specify the settings required to initialize the link (see "Specifying interface settings" on page 46), and to establish a connection to the network (see "Layer 2 testing" on page 46 and "Layer 3 testing" on page 78).

Step4 To Launch the VLAN scan, select the **Toolkit** softkey on the lower right of the Results screen. Then select the **VLAN Scan** button. The VLAN Scan Loading intermediate screen appears followed by the VLAN Scan window.

Step5 Enter the **Duration per ID(s)**. This specifies the length of time (in seconds) for which each VLAN ID will be searched.

Step6 Enter **Number of ranges**- the number of ranges of VLAN ID's you want to be searched.

Step7 Enter **VLAN ID Min** (one for each Range). The minimum value in the range to be searched.

Step8 Enter **VLAN ID Max** (one for each Range). The maximum value in the range to be searched.

Step9 To specify the **Frame size**, **Bandwidth** or the **Pass Criteria**, select the A**dvanced VLAN Scan Settings** link on the lower right corner. Select **Back** when complete to return to VLAN Scan window.

Step10 To run the test, select **Start Test**.

Step11 A progress bar, and the remaining time to test completion, will appear at the top of the screen. To cancel the test at any time press the **Abort Test** button.

Step12 When the test is complete, a dialog box appears asking if you would like to save a test report. For details, see "Saving automated test report data" on page 336.

The VLAN test is complete. The report will provide the total number of VLANs tested, the total number of successes, and the total number of failures. It can also optionally include the test progress log that appeared as you were running the test.

Automated FTP Throughput tests

If your instrument is configured and optioned to do so, you can use it to run the FTP Throughput test. This test is used to transfer files of a known size using FTP, and then measure the actual FTP throughput. When calculating the throughput, the test considers key factors such as the link speed, frame size, latency on the link (delay), and the TCP window size.

For details, contact Customer Care for a copy of the *FTP Throughput Testing* white paper.

To run the FTP Throughput test

Step1 Establish a LAN connection to the network using one of the Ethernet test interfaces on the Transport Module or MSAM. *Do not use the RJ-45 connector provided on the base unit*.

Step2 If you haven't already done so, use the Test Menu to select the Layer 3 or Layer 4 Traffic application for the circuit you are testing (see "TrueSAM" on page 264).

Step3 Specify the settings required to initialize the link (see "Specifying interface settings" on page 46), and to establish a connection to the network (see "Layer 3 testing" on page 78).

Step4 Launch the FTP Throughput test (see "TrueSAM" on page 264), and then wait for the Current Script dialog box to appear. Depending on the number of processes you have running, this may take several seconds.

Step5 Select or create a new configuration for your test. Refer to "Configuring the Enhanced RFC 2544 or Fibre Channel tests" for detailed instructions.

After you select an existing configuration or create a new one, the Configuration Summary dialog box appears listing the current settings for your test.

Step6 To modify the settings, press **Next**.

The Destination Configuration dialog box appears. Specify the Server ID, Login Name, and Password required to establish a connection for the file transfer, and then press **Next**.

The File Configuration dialog box appears.

Step7 Select the sizes of the files that you want to transfer, and then specify number of trials for the transfers. Press **Next** to proceed to the Theoretical Calculation dialog box.

Step8 To estimate the throughput, you must specify a theoretical bandwidth utilized by the link, delay, and if applicable, encapsulation for the simulated traffic. Specify each of these values, and then press **Next**.

The Configuration Summary dialog box appears, listing the settings that you specified.

Step9 Review the settings. If they reflect the scenario that you want to emulate, press **Start** to run the script.

Step10 The FTP Throughput dialog box appears, providing the status of the connection, each of the file transfers, and throughput measurements. See Figure 106.

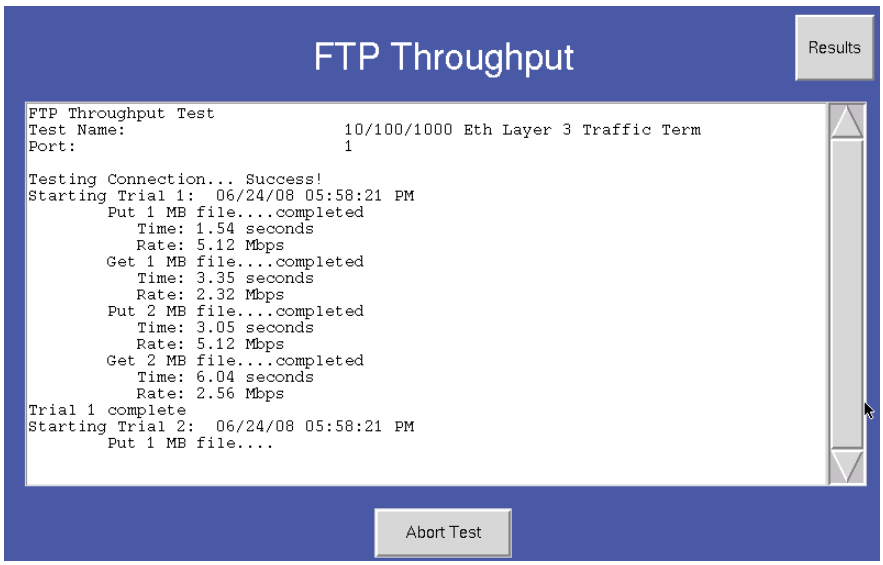


Figure 106FTP Throughput dialog box

When the test is complete, a dialog box appears asking if you would like to save a test report. For details, see "Saving automated test report data" on page 336.

The FTP Throughput test is complete. The report will provide a summary of the parameters that you specified when you configured the test, and then it will provide a summary with the minimum and maximum time in Mbps that it took to send and receive files for each size selected. A table listing theoretical and measured values follows the summaries.

Automated HTTP Throughput tests

If your instrument is configured and optioned to do so, you can use it to run the HTTP Throughput test. This test is used to determine the amount of time it takes to open an HTTP connection, reach a specific web server, and then open the web page.

To run the HTTP Throughput test

Step1 Establish a LAN connection to the network using one of the Ethernet test interfaces on the Transport Module or MSAM. *Do not use the RJ-45 connector provided on the base unit*.

Step2 If you haven't already done so, use the Test Menu to select the Layer 3 or Layer 4 Traffic application for the circuit you are testing (see "Launching a single automated test" on page 279).

Step3 Specify the settings required to initialize the link (see "Specifying interface settings" on page 46), and to establish a connection to the network (see "Layer 3 testing" on page 78).

Step4 Launch the HTTP Throughput test (see "Launching a single automated test" on page 279), and then wait for the Select URL dialog box to appear. Depending on the number of processes you have running, this may take several seconds.

Step5 If the URL you want to connect to appears in the selection box, select it, otherwise, type the URL into the field provided.

Step6 Press **Start**.

The HTTP Throughput Test dialog box appears, providing the status of the connection, a list of the files downloaded to build the web page (such as the style sheet and graphics, and the number of bytes retrieved from the site. The average retrieval rate for the site is also listed (see Figure 107).

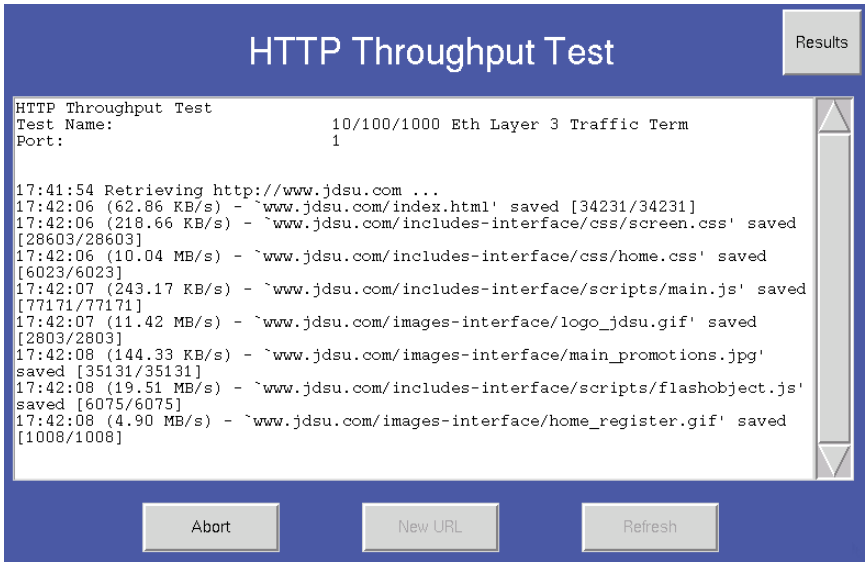


Figure 107HTTP Throughput Test dialog box

You can select **Refresh** to issue a new request for the same web site, or you can select **New URL** to connect to a different site.

When you are done testing, select **Close**. A dialog box appears asking if you would like to save a test report. For details, see "Saving automated test report data" on page 336.

The HTTP Throughput test is complete. The report will list each URL, the number of times you visited it during the test, the size of the site in bytes, and the minimum, maximum, and average rate in Mbps that it took to connect to the site.

Automated TCP Throughput tests

If your instrument is configured and optioned to do so, you can use it to run the TCP Throughput test. This test is used to establish a TCP connection to a peer, and then estimate the maximum TCP throughput on a link for a variety of window sizes (ranging from 8 Kbps to 64 Kbps), when running up to 10000 parallel sessions and factoring in the average delay. The window size represents the maximum number of bytes that can be transmitted before waiting to receive an acknowledgement that the receiving port is receiving frames/packets.

For example, the test may show that, with a current average delay of 10.25 ms, the maximum possible throughput for one TCP session with a window size of 8 Kbps would be 0.098 Mbps.

The average delay value is obtained from the measurement provided in the L2 Link Stats result category.

To run the TCP Throughput test

Step1 If you haven't already done so, use the Test Menu to select the Layer 3 or Layer 4 Traffic application for the circuit you are testing (see "Launching a single automated test" on page 279), and connect the instrument to the circuit. For details, refer to the *Getting Started Manual* that shipped with your instrument or upgrade.

Step2 Specify the settings required to initialize the link (see "Specifying interface settings" on page 46).

Step3 Press **Setup**, and then do the following to configure your test:

- **a** Specify the layer 2 Ethernet settings (see "Layer 2 testing" on page 46).
- **b** Specify the layer 3 IP settings (see "Layer 3 testing" on page 78).
- **c** If you are running a Layer 4 Traffic application, specify the layer 4 TCP settings (see "Specifying layer 4 settings" on page 152).

Step4 Launch the TCP Throughput test (see "Launching a single automated test" on page 279), and then wait for the Estimated TCP Throughput dialog box to appear. Depending on the number of processes you have running, this may take several seconds.

Step5 Estimated throughput for each of the window sizes appear in a tabular format. The number of parallel sessions needed to obtain maximum throughput for each window size is provided at the bottom of the dialog box.

The TCP Throughput test is complete.

TrueSpeed Test

If your instrument is configured and optioned to do so, you can use it to run the TrueSpeed Test. This test uses the Wirespeed application to test the upstream and downstream links for transmission parameters.

There are two distinct functions for which the TrueSpeed test may be used - circuit troubleshooting and circuit turnup. Distinctly different configuration paths are provided for these options.

The following topics are discussed in this section:

– "TrueSpeed test steps" on page 322
– "Initiating the TrueSpeed test." on page 324
– "Configuring the TrueSpeed test" on page 324
– "Running the TrueSpeed test" on page 329

TrueSpeed test steps

If your instrument is configured and optioned to do so, you can use it to run the TrueSpeed Test for the purpose of troubleshooting a circuit experiencing reduced performance or when turning-up a new circuit. This test uses the Wirespeed application and automates TCP throughput testing per the IETF draft standard "ippm-tcp-throughput-framework" and to allow TCP throughput testing for up to 64 connections. Unlike the RFC 2544 test which uses layer 2/3, this test uses layer 4. The troubleshooting option validates that the network is tuned as expected, verifies prioritization of services, and can eliminate finger-pointing between the end user and the network provider.

In addition, the more basic turn-up testing, is a mostly automated test that provides push-button pass/fail testing of a newly installed circuit. The upload and download CIR's need to be added to the configuration before it is run. These parameters can be obtained from the RFC 2544 test that is often run immediately prior to a TrueSpeed Test.

NOTE:

TrueSpeed is run in the turnup mode when activated as a component test of the TrueSAM automated test sequence.

About the test steps

Per the IETF draft standard, this test includes five steps, described in the following section.

In the turnup option, the test is configured to run the Path MTU (if user-selected), RTT, Walk the Window and TCP throughput steps (Steps 1, 2, 3 and 4). Bidirectional tests can only be run in this mode.

When troubleshooting an existing circuit, it is recommended that the user run all five steps for the first test and then run specific tests to further diagnose issues. This is because the automated test uses results from prior steps (i.e. RTT) as input for subsequent steps and eliminates much of the manual configuration.

IMPORTANT NOTE:

In troubleshooting mode, a 6000 Server or Iperf server must be active and the 6000 Client (the 6000 running the automated test), must be configured to communicate with the IP of the Server. This is specified in the Connect configuration tab (step 2 of "TrueSpeed Circuit Turnup Option" on page 325 and step 1 of "TrueSpeed Circuit Troubleshooting Option" on page 327).

Step 1: Determine the path MTU

Packetization Layer Path MTU Discovery (PLPMTUD) is a method for TCP to dynamically discover the MTU of a path by probing with progressively larger packets. It resolves many of the robustness problems of the classical techniques (PMTUD) since it does not depend on the delivery of ICMP messages.

The general strategy is for the Packetization Layer to find an appropriate Path MTU by probing the path with progressively larger packets. If a probe packet is successfully delivered, then the effective Path MTU is raised to the probe size. The packet probe size is raised until the packets fail to be delivered; this implies that the IP “Do Not Frag” (DF) bit is set on all packets.

Step 2: Determine the baseline RTT

Before stateful TCP testing can begin, it is important to baseline the round trip delay and bandwidth of the network to be tested.

These measurements provide estimates of the ideal TCP window size, which will be used in subsequent test steps.

This test is equivalent to a “TCP Ping” and transfers a light load TCP traffic stream from the client to the server and provides RTT values.

Step 3: Run an enhanced walk the windows scan

This step runs the traditional Walk the Window test with four different window sizes, but the Results screens are enhanced to show measured versus expected throughput results in troubleshooting mode if the RTT test was also selected.

Step 4: Measure TCP throughput

This step estimates and measures the maximum TCP throughput on a link for a specific window size and allows the user to specify a file size to transfer between the client and the server.

This test produces a throughput dashboard result screen which clearly shows the expected versus measured TCP throughput along with key loss and delay related metrics. For the more advanced user, throughput versus loss and delay graphs are also available.

Step 5: Evaluate traffic shaping

In most cases, the network connection between two geographic locations (such as branch offices) is slower than the network connection of the host computers. An example would be LAN connectivity of GigE and WAN connectivity of 100 Mbps. The WAN connectivity may be physically 100 Mbps or logically 100 Mbps (over a GigE WAN connection). In the later case, rate limiting is used to provide the WAN bandwidth per the SLA.

This step evaluates traffic shaping. Simply stated, traffic policing marks and/or drops packets which exceed the SLA bandwidth (in most cases, excess traffic is dropped). Traffic shaping employs the use of queues to smooth the bursty traffic and then send out within the SLA bandwidth limit (without dropping packets unless the traffic shaping queue is exceeded).

Traffic shaping can provide improved TCP performance since the retransmissions are reduced, which in turn optimizes TCP throughput for the given available bandwidth.

The ability to detect proper traffic shaping is more easily diagnosed when conducting a multiple TCP connection test. Proper shaping will provide a fair distribution of the available bottleneck bandwidth, while traffic policing will not. The traffic shaping evaluation builds upon the concepts of testing multiple connections.

This test provides graphical test results which visually indicate whether the bottleneck link is traffic shaped or policed.



NOTE

Traffic shaping not applicable to stand-alone Wirespeed applications, any IPv6 application or within Sam Complete.

Initiating the TrueSpeed test.

There are two ways to initiate the TrueSpeed test; both from the Select Test application tree.

– Select the interface and technology for the Layer 4 TCP Wirespeed application you desire. Then initiate the TrueSpeed test using the on-screen softkey.

– Select the TrueSpeed implementation of Layer 4 TCP Wirespeed application on the technology and interface you want to use.

The first option will be necessary if you have no configurations saved to load the parameters of the TrueSpeed test to be run. Alternatively, if you are coming back to run a saved configuration (or modify an existing profile) you can select the direct initiation of the TrueSpeed test, load the existing profile and start testing. For more information see “Launching a single automated test” on page 279.

Launching the TrueSpeed test from L4 TCP Wirespeed application

Step1 Verify that the local and remote instrument are using the same firmware rev. The test may not provide the expected result if the versions are different.

Step2 If not already selected, use the Test Menu to select the L4 TCP Wirespeed application for the interface you are testing. Refer to Table 28 on page 281 for a list of applications.

Step3 If troubleshooting a circuit, verify that a TCP Server (such as another 6000A running TCP Wirespeed) is activated or an Iperf server is available, and that the IP address is specified. This will be automatically confirmed in turnup mode.

Step4 On the right side of the main screen, select **TrueSpeed Test** soft button.

Step5 The Test Configuration options screen appears.

Configuring the TrueSpeed test

Configuration of the TrueSpeed test can be broken into two segments. The first segment is common to all configurations and the second is specific for the turnup option or the troubleshooting option.

When the True Speed application initializes the Configure screen appears. There are two options for configuring TrueSpeed:

– To configure all options yourself, select the green arrow to the right of **Configure Test Settings Manually**. Go to step 2.

– To load configuration settings set from a previously saved file select the green arrow to the right of **Load Configuration from a Profile**.

Step1 The Profile selection window appears.

The filenames of the saved profiles will be listed on the left side of the screen and all sections of the currently loaded profile will be listed on the right side of the screen.

Do the following:

a Select a profile from the list whose configuration is to be loaded.

b Check those sections, on the right side of the screen, that are to be loaded into the test. If no profile has yet been selected, the currently configured profile sections will be checked.

Any section not selected will not be configured into the test. Any parameter of the test (checked or not checked) may be reconfigured at a later point in the configuration process.

c Select the **Load Profiles** button to load all checked sections into the test. After profile has successfully loaded, select **OK** and then select the **Next** arrow. Go to "Running the configured TrueSpeed test" on page 329.

Step2 The Mode Selection screen appears.

Do one of the following:

– To continue with troubleshooting, select the radio button for **troubleshooting**. Go to "TrueSpeed Circuit Troubleshooting Option" on page 327.

– To proceed with a circuit turnup, select the radio button for **installing** or **turning-up.** Continue to "TrueSpeed Circuit Turnup Option".

TrueSpeed Circuit Turnup Option

Step1 The Symmetry selection screen appears. Select the radio button for a symmetrical circuit (My downstream and upstream throughputs are **the same**) or asymmetrical (My downstream and upstream throughputs are **different**). Then select **Next** (the green arrow).

Step2 The Connect:Channel screen appears (see Figure 108).

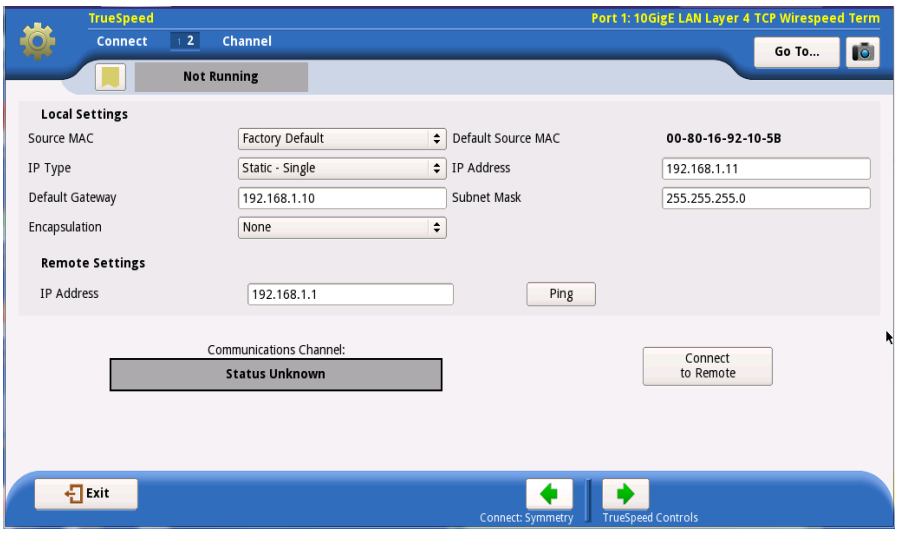


Figure 108 TrueSpeed Turnup Connection Settings

Do the following:

a In the Local Settings portion of the window, define the parameters of the local connection including MAC, IP addresses and encapsulation, if any.

b In the Remote portion of the window, define the IP address of the remote connection. To verify that there is a device at the address specified, select the **Ping** button. If there is a device, a green check mark will appear beside the Remote IP address.

c To establish a valid connection for running the test, select the **Connect to Remote** button. When the connection is determined to be valid, the bars for **Local Port**, **Auto Negotiation**, and **Communications Channel** will turn yellow and then green when communication is established. The bars will display messages indicating the status of the connection operation.

If the connection is invalid, a message window will appear providing some information as to why the connection is invalid. This connection issue must be resolved before the test can be run, although configuration may continue.

To continue with the configuration, select the green arrow on the right at the bottom of the screen (legend text will vary whether the connection has been made or is to be skipped).

Step3 The TrueSpeed Controls window will appear (see Figure 109 and Figure 110).

This window provides for the configuration of the parameters pertaining to the Committed Information Rate (CIR) and TCP Threshold, among others, which will be used on all subsequent TrueSpeed tests. IF Traffic shaping is selected, CIR=L1 Committed Information Rate

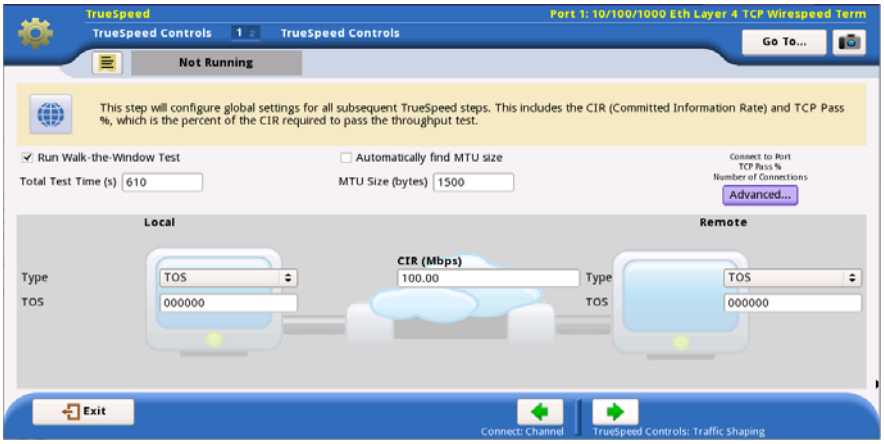


Figure 109 TrueSpeed Symmetrical Turnup Configuration

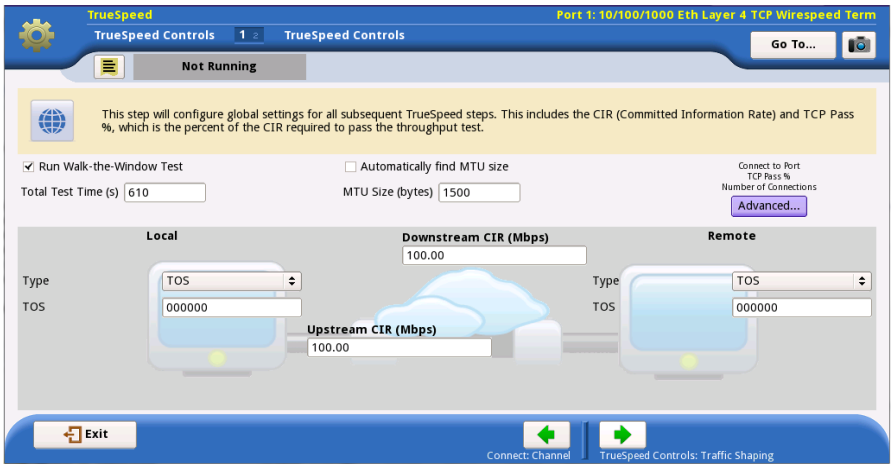


Figure 110 TrueSpeed Asymmetrical Turnup Configuration

The Advanced button provides access to additional parameters to define the **Port Connection**, **TCP Pass %**and whether **Multiple Connections** are desired. When these have been defined, select the **Back** (left green) arrow.

After all parameters have been specified, select **Next** (the green arrow).

Step4 Depending on the application being run, the following screen may ask whether you want to shape the TCP traffic.

– To run the test without shaped traffic testing select the **No** radio button. Select Next (green arrow). Got to step 5.

– To run the test with shaped traffic select the **Yes** radio button. This option will run the test with traffic shaping and then without to provide a comparison of TCP throughput for both conditions.

– If you need to specify the **Tc** and **Bc** values before running the test, select the **Advanced** radio button. When in the Advanced mode shaping can be selected for the local or remote unit individually. This level of control is available by checking the **Show additional testing options** checkbox.

When all options are as desired, select Next (green arrow).

NOTE

When traffic shaping is selected, the Committed Information Rate (CIR) will be the L1 CIR.

Step5 The Save Profiles window appears.

If no Profile is to be saved at his time, select the **Skip Profiles** arrow at the bottom of the window. Go to "Running the TrueSpeed test" on page 329

If it is desired that the configuration be saved to memory (disk or USB), specify the filename and the location where it is to be stored. If it is desired that subsequent users be restricted from being able modify this profile, check the box **Save as read-only.**

To save the file to memory, select the **Save Profiles** button. Then select **Next** (the green arrow). The test will begin. Go to step 3 on page 330.

TrueSpeed Circuit Troubleshooting Option

Step1 The Connection Channel screen appears.

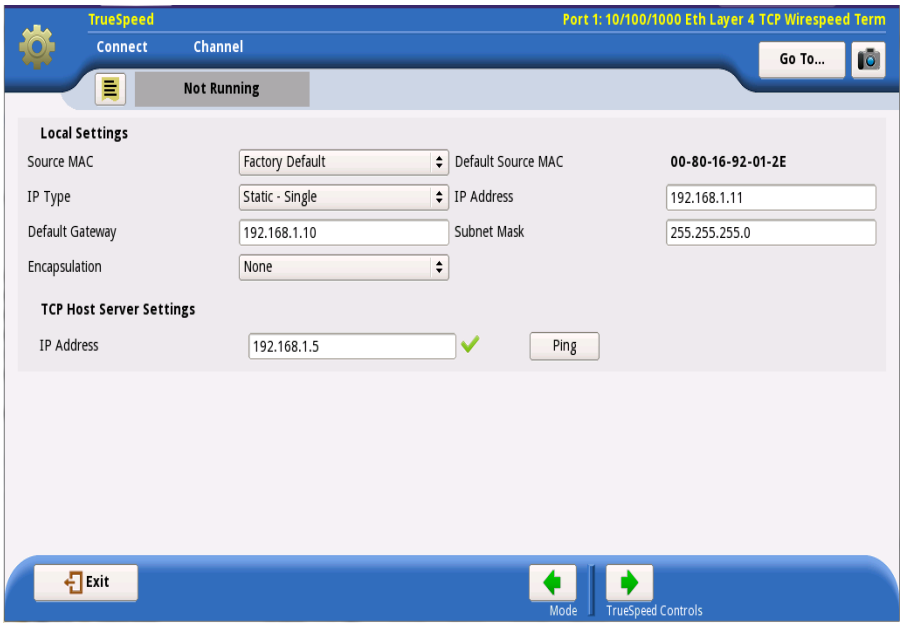


Figure 111 TrueSpeed Troubleshooting Connection Settings

NOTE:

All settings will be set to defaults upon selecting the troubleshoot mode.

Do the following:

a In the Local Settings portion of the window, define the parameters of the local connection including MAC, IP addresses and encapsulation, if any.

b In the TCP Host Server Settings portion of the window, define the IP address of the TCP host server. To verify that there is a device at the address specified, select the **Ping** button. If there is a device, a green check mark will appear beside the Remote IP address.

c To continue with the configuration, select the select Next (right green arrow)- at the bottom of the screen.

Step2 The TrueSpeed Controls window will appear (see Figure 112).

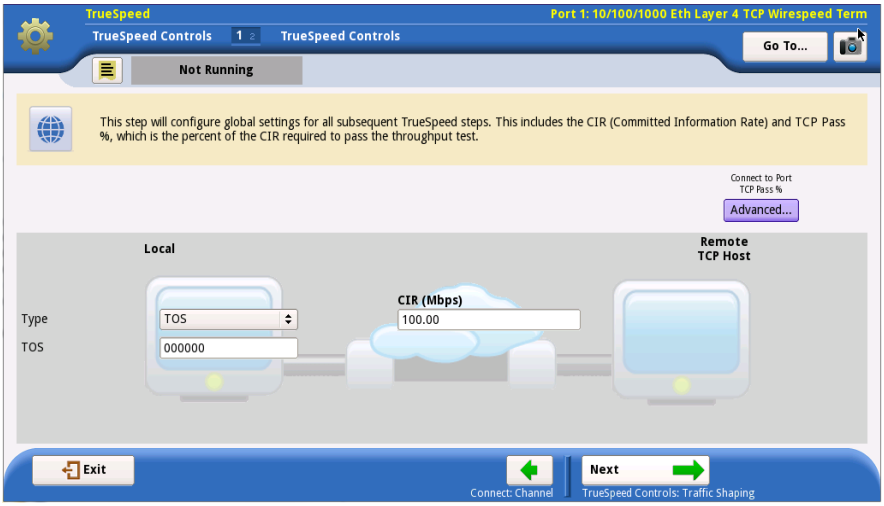


Figure 112 TrueSpeed Troubleshooting Controls Configuration

This window provides for the configuration of the parameters pertaining to the Committed Information Rate (CIR) and TCP Threshold, among others, which will be used on all subsequent TrueSpeed tests.

Step3 Depending on the application being run, the following screen may ask whether you want to do shape the TCP traffic.

– To run the test without shaped traffic testing select the **No** radio button. Select Next (green arrow). Got to step 4.

– To run the test with shaped traffic select the **Yes** radio button. This option will run the test with traffic shaping and then without to provide a comparison of TCP throughput for both conditions.

– If you need to specify the **Tc** and **Bc** values before running the test, select the **Advanced** radio button. When in the Advanced mode shaping can be selected for the local or remote unit individually. This level of control is available by checking the **Show additional testing options** checkbox.

After all parameters have been specified, select **Next** (the green arrow).

Step4 The Step Configuration window appears.

Select the steps that are to be included in the TrueSpeed test. To learn more about each step, see “About the test steps” on page 322. When all desired steps are chosen, select **Next** (the green arrow).

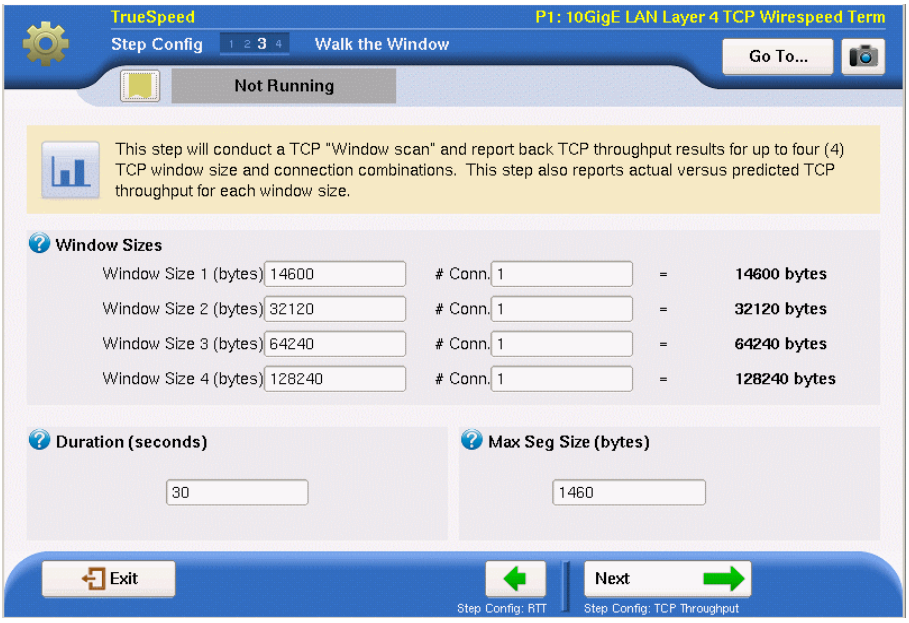
Step5 If selected, the Path MTU window appears.

Specify the **MTU Upper Limit** (this value represents the starting point - the upper value - with which the test set will begin the Path MTU search). Then select **Next** (the green arrow).

Step6 If selected, the RTT window appears.

Enter the **Duration** of the Round Trip Delay test (this test will calculate the inherent latency of the network) in seconds. Then select **Next** (the green arrow).

Step7 If selected, the Walk the Window screen appears.



Specify the test **Window Size**s, **# Conn**ections to each window and **Test Duration** (and **Max Segment Size** in bytes if Path MTU is not selected).Select **Next** (the green arrow).

Step8 The TCP Throughput window appears.

Specify the **Window Size** (in bytes), **File Size per Connection** or check box to **Automatically find file size for 30 second transmit** and **Number of Connections** (and the **RTT** (in ms) and **Max Segment Size** (in bytes) if RTT and Path MTU are not selected).Then select **Next** (the green arrow).

Step9 If the Advanced TCP Test has been selected, the Advanced TCP window appears.

Specify the **Test Duration** (and **Window Size** and **Number of Connections** if the RTT step is not selected). Then select **Next** (the green arrow).

Step10 The Save Profiles window appears.

Do one of the following:

a If no Profile is to be saved at his time, select the **Skip Profiles** arrow at the bottom of the window. Go to “Running the TrueSpeed test” on page 329.

b If it is desired that the configuration be saved to memory (disk or USB), specify the filename and the location where it is to be stored. If it is desired that subsequent users be restricted from being able modify this profile, check the box **Save as read-only.**

To save the file to memory, select the **Save Profiles** button. Then select **Next** (the green arrow). Go to “Running the TrueSpeed test” on page 329.

Running the TrueSpeed test

When the TrueSpeed test has been completely configured three options are available - run the test as configured, reconfigure the test (possibly to save as a different profile) or load a saved profile (except when profile has just been loaded).

Running the configured TrueSpeed test

Step1 The Run/Edit window appears.

To return to the beginning and modify existing configuration, select the **Go** arrow after “Change Configuration”. Go to step 2 of “Configuring the TrueSpeed test” on page 324.

To load a previously saved set of configuration parameters, select the **Go** arrow after “Load Configuration from a Profile” (or left green arrow at the bottom of the window if coming from Profile Selection). Go to step 1 in “Configuring the TrueSpeed test” on page 324.

To run the test, as configured, select the **Go** arrow after “Select and Run Tests”.

Step2 The Run TrueSpeed Tests window appears.

The blinking button labeled Run Test indicates that the test is not yet running. To start the test, press the **Run Test** button. The button will change to a yellow background and the legend will change to Stop Test.

While running the turnup version of TrueSpeed, a time remaining indication will be shown after the MTU test has been completed. The troubleshooting version indicates its activity by the display of an animated Running indicator.

To abort the test, press the **Stop Test** button.

When the test has completed, if the turnup option had been selected, the screen will show a pass/fail indication. For troubleshooting option, it will not. To continue after the test has been stopped or it has finished, select **Next** (the green arrow).

Step3 The post-test window appears.

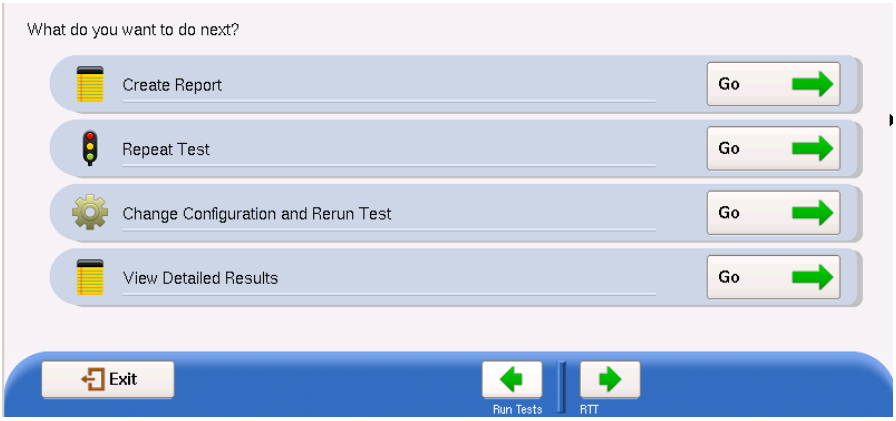


Figure 113 TrueSpeed Post-test Window

If the test fails, a message will appear to help diagnose the cause.

Do one of the following:

– To create a report of the results of the test that just completed, select the **Go** arrow on the “Create Report” line. Go to step 4.

– To repeat the test that just ran, select the **Go** arrow on the “Repeat Test” line. Go back to step 2.

– To reconfigure the test and then run it again, select the **Go** arrow on the “Change Configuration and Rerun Test” line. Go to step 2 of “Configuring the TrueSpeed test” on page 324.

– To view detailed results of the performance achieved during the test, select the **Go** arrow on the “View Detailed Results” line.

  The detailed results are presented on a sequence of windows that vary depending upon the steps in the test that were selected to be run.

  On the last page of the results select the right-pointing green arrow. Go to step 6.

Step4 The Report Info window appears.

Enter the desired information into the fields and identify the location of a logo that should be added to the report. When all desired information has been defined, select **Next** (the green arrow).

Step5 The Report window appears.

Identify the location where the report is to be saved, the format of the report and the file-name in which to save it.

You may view the report before and/or after its creation by selecting the **View Report** button and/or checking the “View report after creation” checkbox. The report will automatically load into the appropriate reader (if available) depending upon the format in which it has been saved.

When ready to save the report, select the **Create Report** button. After it has been saved (and viewed), select the right-pointing green arrow.

Step6 The post-report/results window appears.

All options available on this window are described in step 3 with the exception of the “Exit TrueSpeed test”.

To exit the TrueSpeed application, select the **Go** arrow after “Exit TrueSpeed test”.

Step7 The Exit window appears.

Do one of the following:

- To start the TrueSpeed test from the beginning, select the **Start Over** button. Go to“Configuring the TrueSpeed test” on page 324.
- To restore the configuration setups to their default values when leaving the application, check the box **Restore Setups on Exit**.
- To exit to the base application, retaining all setups from the TrueSpeed test, select the Exit to Results button.
- To return to the previous window, select **Cancel**.

The TrueSpeed test is finished.

Testing using TAM automation

If your instrument is configured and optioned to do so, you can use it to remotely log into and provision network elements (for example, switches and routers) from a Mobility Switching Center (MSC) by issuing TL1 commands (See Figure 114).

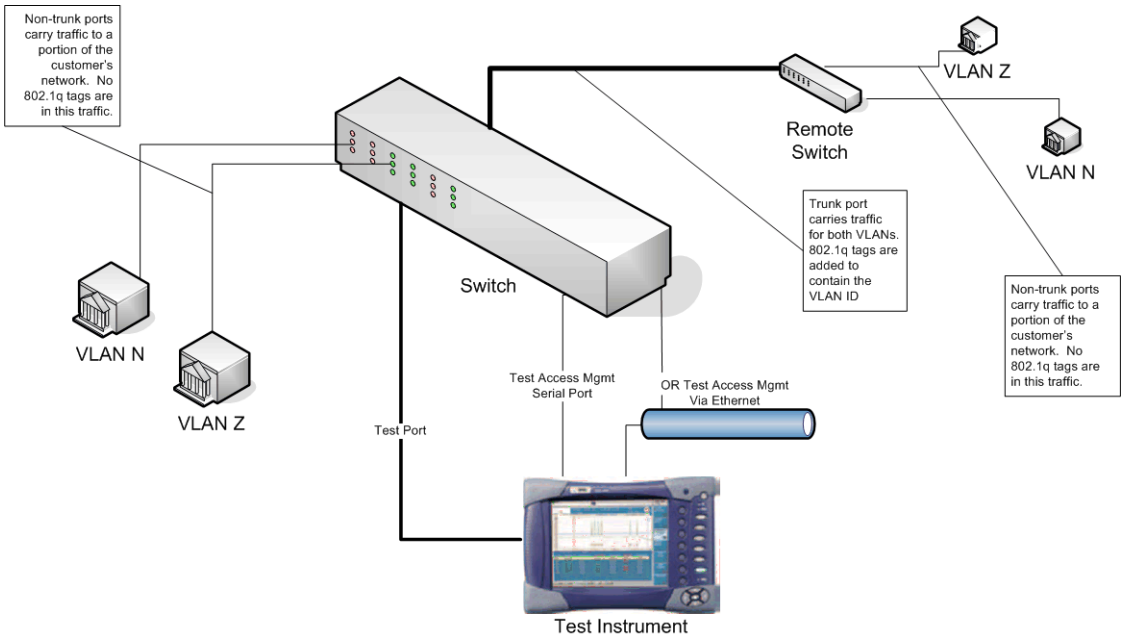


Figure 114 Provisioning NE using TAM

You can also use it to emulate a router on the network end of the Ethernet Transport Service (ETS), then run an RFC 2554 script (see "Automated RFC 2544 and Fibre Channel tests" on page 282). The script puts a Network Interface Device (NID) in loop back mode, then transmits traffic from the instrument. The NID loops the traffic back to the instrument, where you can analyze results for the traffic to determine link characteristics such as throughput and latency.

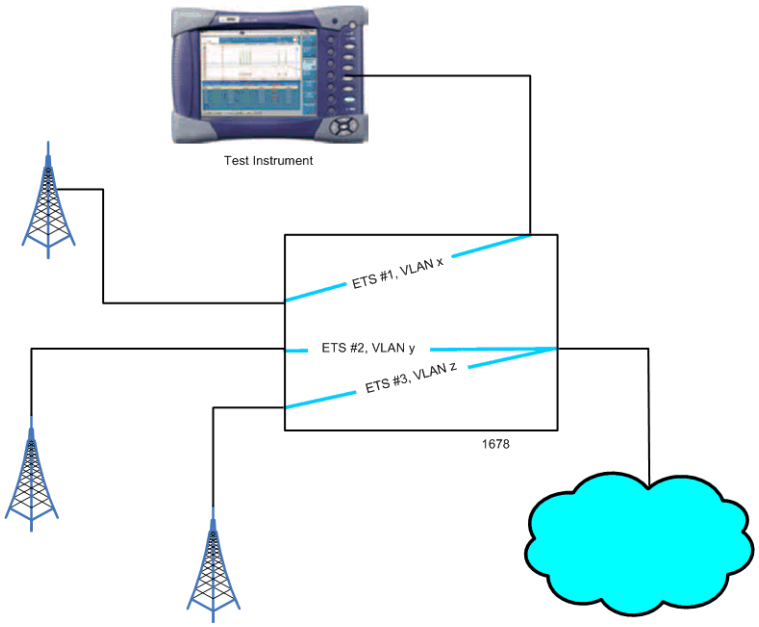


Figure 115 Router emulation configuration

Before testing

Before connecting to an NE using the TAM tool, establish a Username and Password for the test instrument. Be certain to grant privileges that allow the instrument to:

– View the NE's cross-connect definitions.
– Delete cross-connect definitions.
– Activate specific ingress and egress flows in the command line interfaces (CLIs) for the switch ports.

Connecting to the management network

Before running a TAM test, you must connect the instrument to the management network that the NE resides on using the Ethernet management port on your instrument and a straight through Ethernet cable.

To connect the instrument to the network

Step1 Insert one end of a straight through Ethernet cable into the Ethernet management port on your instrument.

– On the MTS/T-BERD 6000A base unit, the port is located on the top panel of the base unit, in the left corner, adjacent to the two USB ports (see Figure 116).



Figure 116MTS/T-BERD 6000A Ethernet Management Port

– On the MTS/T-BERD 8000, the port is located on the top panel of the base unit, in the middle, adjacent to the DB-9 serial port (see Figure 117).

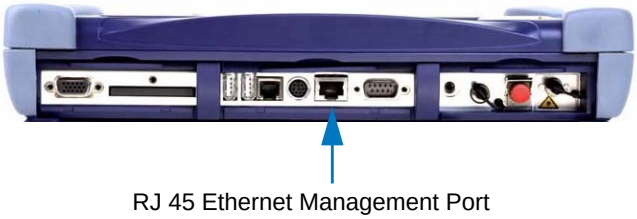


Figure 117MTS/T-BERD 8000 Ethernet Management Port

Step2 Connect the other end of the cable to the access port on the management network that the NE resides on.

The instrument is physically connected to the network. To establish a complete connection proceed to "Setting up a TAM test" on page 334.

Connecting to the test network

In addition to the management connection, you must establish a connection for the traffic transmitted by the instrument and received from the network element.

The ports and cables used to connect the instrument to the circuit for testing vary depending on the line rate of the test interface. For details on connecting the instrument to the circuit for testing, refer to the *Getting Started manual* that shipped with your instrument or upgrade.

Setting up a TAM test

Before monitoring or configuring a network element using the Test Access Management tool, (TAM), you must specify the settings required to establish a connection to the NE, indicate the test mode (Monitor or Emulate), and provide the ingress and egress flow.

To specify the TAM settings

Step1 If you haven't already done so, use the Test Menu to select the Layer 2 or Layer 3 Traffic application for the circuit you are testing (see "Launching a single automated test" on page 279), and connect the instrument to the circuit. For details, refer to the *Getting Started Manual* that shipped with your instrument or upgrade.

Step2 On the Main screen, select the **Toolkit** softkey, then select **TAM Setup**.

The TAM Setup screen appears, with tabs that allow you to specify connection settings and test port settings. Tabs are also provided that allow you to observe the status of the connection, and the version of the TAM application currently running on your instrument.

Step3 On the **Connection** tab, specify the following settings:

Setting	Value
Network Element Type	Select the type of NE that you are monitoring or configuring.
Network Element IP Address	Enter the IP address for the NE.
Network Element IP Port	Enter the port identifier for the NE's *management port*. Note: When Network Element Type is set to SSH, the port will be set to **22**. When Network Element Type is set to Telnet, the port will be set to **23**.
Username	Enter the username you created for the test instrument. This name is used to log on to the NE and to ensure that the instrument is authenticated for TAM testing.
Password	Enter the password required to log on to the NE.
Login type	Select from SSH (port = 22) or Telnet (port=23). Only applicable when NE type = Alcatel 7750, 7450 or 7705.

Step4 Select the **Test Port** tab, then specify the following settings:

Setting	NE Type	Value
Method	Any	Indicate whether you intend to monitor the NE, or emulate a router on the network end of an ETS. Note- If the NE was specified as Alcatel 7705 then only **Emulate** will be available
Test Port	Any	Enter the port identifier for the port that your instrument is connected to for *testing* (this is not the same port specified as the NE's management port). – If the NE Type is 167x, the port ID must be in a #/p#/p# format, where the last /p# is optional. – If the NE Type is 7x50, the port ID must be in a #/#/# format.
Test VLAN	Any	Enter the VLAN ID carried in the traffic transmitted or monitored on the instrument's test port when the instrument is *emulating a router*.
Ingress Flow	Alcatel 1675 Alcatel 1678	Enter the name of the inbound flow.
Egress Flow	Alcatel 1675 Alcatel 1678	Enter the name of the outbound flow.
Service ID	Alcatel 7750 Alcatel 7450	Enter the ID for the epipe.
Customer Port	Alcatel 7750 Alcatel 7450	Enter the port identifier for the customer port.
Customer VLAN	Alcatel 7750 Alcatel 7450	Enter the VLAN ID for the customer port.

Step5 Use the buttons at the bottom of the screen to do the following:

Button	Appears ...	Used to ...
Configure	At all times	Configure the NE port with the values you specified, and take you to the Status tab. The NE IP address must be specified before the port can be configured.
Restore	At all times	Restore the NE's original configuration values and takes you to the Status tab.
Exit	At all times	Exit the TAM script.
Upgrade	If the TAM script is launched and the instrument detects an upgrade on an attached USB key.	Install a detected upgrade from a USB key and take you to the Status tab.

The TAM settings are specified. After a connection is established, you can use the TAM script to configure and monitor the network element. You can observe the status of each command executed on the Status tab. The current version of the TAM server software appears on the Version tab.

For details on using TAM automation, refer to the *QT-600 Ethernet and Triple-Play Probe User Interface Guide*.

Saving automated test report data

When each automated test is complete, a dialog box appears asking if you would like to save a test report. You can optionally append the progress log (the text that appeared while you were running the test) to the end of the report.

To save automated test report data

Step1 When the report dialog box appears, if you would like to append a progress log to the end of the report, select the option on the dialog box, then reply with **Yes** or **No**. If you select Yes, specify the following:

- The customer's name.
- Your name.
- Work Order No.
- The test location.
- Any additional comments you might have concerning the test.

Select the right-facing green arrow. The Report screen appears.

Step2 This screen allows two actions - Generating a report of the most current results or viewing a previously saved report. To generate a new report:

a Select the radio button for the format desired.

b Change the default file name, if desired, or click on the Select button to open the report file management screen to find existing file names. To overwrite an existing file, select it from the list and then click the Select button to return to the Report screen.

c To display the report on the screen after it is generated, check the View report after creation checkbox.

d To include the message log in the generated report, check the Include message log checkbox.

e Select the Create Report button.

Step3 To View previously saved report;

a Select the create Report Button. The View Report screen appears.

b from this screen you can see the list of currently saved reports in available locations. To view an existing report, select its filename then, click on View. the report will display on the screen.

c When finished with the report, select the Exit button to return to the Report screen.

Step4 When completed with the Reports, select the left-facing green button to re-specify your report or the Exit button.

The Exit screen appears.

Step5 To restore the setups to their previous settings, check the Restore Setups on Exit checkbox.

Step6 To return to the base application, select the Exit button.

Step7 To return to the Report screen, select the Cancel button.

Step8 Select **Close** to close the dialog box and return to the Main screen.

The report is saved.



NOTE:

You can not view Chinese or Japanese PDFs on your test instrument. if you save the report in a PDF format, you must export the PDF, then load it onto a PC or workstation with a PDF Viewer.

If you need to view Chinese or Japanese reports on the test instrument, save the report data as an HTML file.

13

Test Results

This chapter describes the categories and test results that are available when performing Ethernet, Fibre Channel, TCP/UDP, and IP Video tests. Topics discussed in this chapter include the following:

– “About test results” on page 340
– “Summary Status results” on page 340
– “CPRI/OBSAI test results” on page 341
– “Ethernet, IP, TCP/UDP, and Fibre Channel results” on page 345
– “Wander Interface results” on page 396
– “IP Video results” on page 397
– “VoIP results” on page 408
– “Graphical results” on page 413
– “Histogram results” on page 414
– “Event Log results” on page 414
– “Time test results” on page 415

About test results

After you connect the instrument to the circuit and press the START/STOP button, results for the configured test accumulate and appear in the Result Windows in the center of the screen. The result groups and categories available depend on their applicability to the test you configured. For example, if you select, configure, and start a SONET test application, 10 Gigabit Ethernet LAN categories are not available because they are not applicable when running a SONET application.

A number of enhancements have been made to the test result layout; for details, see “Step 5: Viewing test results” on page 4.

The following sections describe the test results for each of the categories.

Summary Status results

When running most applications, the Summary Status category displays a large “ALL SUMMARY RESULTS OK” message on a green background if no errors, anomalies, alarms, or defects have been detected (see Figure 118).

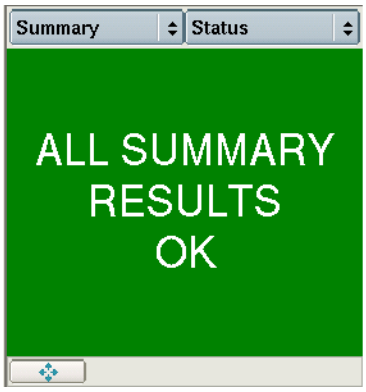


Figure 118ALL SUMMARY RESULTS OK message

If errors, anomalies, alarms, or defects *have* been detected, the background is red, and the errored results are displayed (see Figure 119).

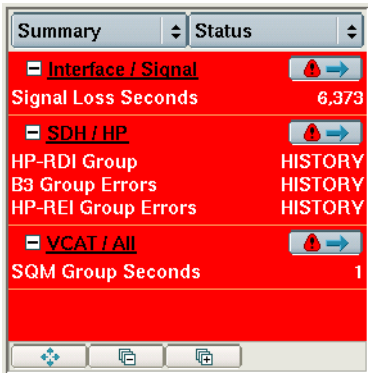


Figure 119 Errored Summary Status results (NextGen application)

This allows you to immediately view errored results without searching through each category. The errored results are listed by group and category. To see all results for the group/category, select the arrow key to the right of the group/category name. You can also collapse or expand the results by selecting the box to the left of the name.

If OoS (out of sequence) Layer 3 Packets, B8ZS Detect, Path Pointer Adjustment, or correctable FEC conditions occur, and *no other errors occurred*, the background is yellow, indicating you should research each condition displayed. In some instances, the conditions constitute errors; in other instances, the conditions are expected and should not be interpreted as errors.



IP VIDEO RESULTS:

When running IP Video applications, the Summary Status results provide a layered view of the state of the physical/link, transport stream, and video stream quality layers. For details, see “IP Video results” on page 397.

CPRI/OBSAI test results

BERT results pertaining to frequency characteristcs, code violations and sync and pattern errors are reported in the results pane on the UI when using Layer 1 applications.

Layer 2 applications additionally report on framing errors and other CPRI specific data.

Categories discussed in this section include the following:

– “CPRI and OBSAI LEDs” on page 341
– “Interface/Signal results” on page 342
– “CPRI/OBSAI Error Stats” on page 343
– “CPRI/OBSAI Counts results” on page 343
– “CPRI L1 Inband Protocol results” on page 344
– “CPRI/OBSAI Payload BERT results” on page 345

CPRI and OBSAI LEDs

If the instrument loses any of the LED events, the green Status LED extinguishes, and the red Alarm LED in the history column illuminates indicating an error condition has occurred.

Table 30 describes the LEDs, and indicates whether each LED is applicable when testing a CPRI or OBSAI circuit.

Table 30 CPRI/OBSAI LEDs

LED	Indicates	CPRI	OBSAI
SIgnal Present	Green – A signal is present. Red – Received signal has been lost since the last test start or restart.	√	√

Table 30 CPRI/OBSAI LEDs

LED	Indicates	CPRI	OBSAI
Sync Acquired	Green – Synchronization is established. Red – Synchronization has been lost since the last test restart.	√	√
Frame Sync	Green – Frame alignment has been achieved. Red – Frame alignment has been lost.	√	√
Pattern Sync	Green – Synchronization with the received test patterns has been achieved. Red – Synchronization has been lost since the last test restart.	√	√

Interface/Signal results

Table 31 describes the CPRI and OBSAI Interface/Signal results.

Table 31 CPRI/OBSAI Interface/Signal Results

Test Result	Description
Optical Rx Level (dBm)	Displays the receive level in dBm when testing optical interfaces using average power consumption.
Optical Rx Overload	Displays current status of Optical Rx Overload condition (On/Off)
Rx Frequency (Hz)	Frequency of the clock recovered from the received signal, expressed in Hz.
Rx Freq Deviation (ppm)	Current received frequency deviation. Displayed in PPM.
Rx Freq Max Deviation (ppm)	Maximum received frequency deviation.
Signal Losses	Number of times signal was lost during current test.
Signal Loss Seconds	Number of seconds during which a signal was not present.
Sync Loss Seconds	Number of seconds during which a synchronization was not present.
Tx Clock Source	Shows the source of the transmit timing standard
Tx Frequency (Hz)	Current transmitter clock frequency, expressed in Hz.
Tx Freq Deviation (ppm)	Current transmitted frequency deviation. Displayed in PPM.
Tx Max Freq Deviation (ppm)	Maximum transmitted frequency deviation.

CPRI/OBSAI Error Stats

Table 33 shows the CPRI/OBSAI Error Stats test results.

Table 32 CPRI/OBSAI Error Stats results

Word Sync Loss Events	A count of the number of word sync loss events that have occurred since the last restart.
Word Sync Loss Seconds	A count of the number of seconds in which a 10b word loss occurred since the last restart
Code Violations	The number of code violations that have been received since the last test restart.
Code Violations Rate	The ratio of code violations to bits received since the last test restart.
Code Violations Seconds	The number of seconds in which code violations have been received since the last test restart.
Rx K30.7 Words	The number of K30.7 words received since the last test restart.
Frame Sync Loss Events	The number of frame sync losses that have been recorded since the last test restart.
Frame Sync Loss Seconds	The number of seconds in which frame sync losses have been received since the last test restart.
Running Disparity Errors	The number of Running Disparity Errors received since the last test restart.
Running Disparity Error rate	The rate at which Running Disparity errors have been received since the last test restart
Running Disparity Error Seconds	The number of seconds in which a running disparity error was received since the last test restart.

CPRI/OBSAI Counts results

Table 33 shows the CPRI/OBSAI Counts results.

Table 33 CPRI/OBSAI Counts results

Rx Code Words	The total number of 10b code words received since last test restart.
Tx Code Words	The total number of 10b code words transmitted since last test restart.
Rx Frames	The total number of hyperframes (CPRI) or master frames (OBSAI) received since last test restart.
Tx Frames	The total number of hyperframes (CPRI) or master frames (OBSAI) transmitted since last test restart.
Rx Message Groups	A count of the number of different groups received.
Round Trip Delay, Current (µs)	The currently calculated round trip delay, expressed in microseconds.
Round Trip Delay , Avg (µs)	The average round trip delay over the last second, expressed in microseconds.
Round Trip Delay , Max (µs)	The minimum round trip delay since the last restart of the test, expressed in microseconds.
Round Trip Delay Min (µs)	The maximum round trip delay since the last restart of the test, expressed in microseconds.

Table 33 CPRI/OBSAI Counts results

Rx Messages	A count of the messages received in each of the following groups- – Control – Measurement – WCDMA/FDD – WCDMA/TDD – GSM/EDGE – TETRA – CDMA2000 – WLAN – Loop back – Frame Clock Burst – Ethernet – RTT – WiMAX – Virtual HW Reset – LTE – Generic Packet – Multi-hop RTT

CPRI L1 Inband Protocol results

Table 34 shows the CPRI-specific L1 Inband Protocol results.

Table 34 CPRI Counts results

Rx Protocol Version	Received CPRI protocol version.
Rx C&M HDLC Rate	Received HDLC bit rate for the slow C&M channel.
Rx C&M Ethernet Subchannel Number	Received subchannel number at which the control words for the Ethernet channel starts within a hyperframe.
Start-up State	Current state of start-up sequence
Tx Protocol Version	Transmitted CPRI protocol version.
Tx C&M HDLC Rate	Transmitted HDLC bit rate for the slow C&M channel.
Tx C&M Ethernet Subchannel Number	Transmitted subchannel number at which the control words for the Ethernet channel starts within a hyperframe.
Port Type	Current status of port type selection (Master/Slave).

OBSAI Status Results

Table 33 shows the CPRI/OBSAI Error Stats test results.

Table 35 OBSAI Status results

Rx State	Current state of the OBSAI receiver.
R Scrambler Seed	Captured scrambler seed by the receiver.
Rx RP3 Bus FCB Sync	Indicates whether RP3 Bus FCB message has been received
Rx RP3 Bus FCB SFN	Latched RP3 Bus FCB SFN value

Table 35 OBSAI Status results

Rx RP3 Bus FCB C1	Latched RP3 Bus FCB C1 value

CPRI/OBSAI Payload BERT results

Table 36 shows the CPRI/OBSAI payload BERT results.

Table 36 CPRI/OBSAI Payload BERT results

Pattern Sync Losses	Count of the number of times pattern sync was lost since initially acquiring pattern synchronization.
Pattern Sync Loss Seconds	The number of seconds in which pattern sync was lost since initially acquiring pattern synchronization.
Bit Error Rate	The ratio of pattern bit errors to received pattern bits since initially acquiring pattern synchronization.
Bit Errors	Count of the number of bit errors received since initially acquiring pattern synchronization.
(Bit) Errored Seconds	Count of the number of seconds containing bit errors since initially acquiring pattern synchronization.
Error-Free Seconds	Count of the number of seconds containing no bit errors since initially acquiring pattern synchronization.
Error-Free Seconds %	The ratio of Errored Seconds to Error-Free Seconds since initially acquiring pattern synchronization.
Total Bits Received	The total number of bits received since initially acquiring pattern synchronization.
Round Trip Delay - Current (µs)	The currently calculated round trip delay, expressed in microseconds.
Round Trip Delay -Average (µs)	The average round trip delay over the last second, expressed in microseconds.
Round Trip Delay - Minimum (µs)	The minimum round trip delay since the last restart of the test, expressed in microseconds.
Round Trip Delay - Maximum (µs)	The maximum round trip delay since the last restart of the test, expressed in microseconds.

Ethernet, IP, TCP/UDP, and Fibre Channel results

Test results such as link counts, statistics, error statistics, and BER results are available when performing Ethernet, IP, TCP/UDP or Fibre Channel testing.

– If you are testing a 10 Gigabit WAN interface, SONET/SDH test results are also available (see the *PDH, SONET, SDH, NextGen, and OTN Testing Manual* that shipped with your instrument or upgrade.

– If you are testing using VPLS encapsulated traffic, link statistics, link counts, filter statistics, filter counts, and BERT statistics for the customer appear in the associated “Customer” result categories. Link statistics and link counts for the service provider are also provided in “SP” categories.

– If you are testing using MAC-in-MAC (PBB) traffic, link statistics, link counts, filter statistics, filter counts, and BERT statistics for the customer frames appear in the associated “Customer” result categories. Link statistics and counts are also provided for the backbone frames.

– If you are testing using MPLS encapsulated traffic, the standard Layer 2 and layer 3 result categories are provided, and test results associated with MPLS testing appear.
– In all cases, only the results applicable to your test appear in each category. For example, if you are performing a Layer 2 Ethernet test with VLAN tagged traffic, VPLS results and Fibre Channel results do not appear because they are not applicable to your test.

Categories discussed in this section include the following:

– "Ethernet, IP, TCP/UDP, and Fibre Channel LEDs" on page 347
– "Cable Diagnostic results" on page 351
– "SLA/KPI" on page 353
– "Interface results" on page 354
– "L2 Link Stats results" on page 355
– "L2 Link Counts results" on page 359
– "L2 Filter Stats results" on page 361
– "L2 Filter Counts results" on page 365
– "J-Proof (transparency) results" on page 366
– "L2 BERT Stats results" on page 367
– "CDMA Receiver Status results" on page 368
– "CDMA/GPS Receiver Log" on page 368
– "Ethernet OAM Service OAM results" on page 369
– "Ethernet OAM Service OAM MEP Discovery results" on page 371
– "Ethernet OAM L-OAM Modes results" on page 371
– "Ethernet OAM L-OAM Counts results" on page 372
– "Ethernet OAM L-OAM States results" on page 373
– "Ethernet OAM L-OAM Error History results" on page 373
– "L3 Link Stats results" on page 374
– "L3 Link Counts results" on page 375
– "L3 Filter Stats results" on page 376
– "L3 Filter Counts results" on page 377
– "L3/IP Config Status results" on page 377
– "Ping results" on page 378
– "Traceroute results" on page 379
– "PCS Error Stats" on page 379
– "Ethernet Per Lane results" on page 380
– "Error Stats results" on page 381
– "Capture results" on page 385
– "Sync Status Messages" on page 386
– "AutoNeg Status results" on page 386
– "Login Status results" on page 388
– "PTP Link Counts results" on page 390
– "PTP Link Stats results" on page 391
– "PTP Graphs" on page 393
– "L4 Link Stats results" on page 393
– "Detailed L4 Stats" on page 393

– "Cumulative L4 results" on page 394
– "L4 Link Counts results" on page 395
– "L4 Filter Stats results" on page 395
– "L4 Filter Counts results" on page 395
– "J-Profiler results" on page 395

Ethernet, IP, TCP/UDP, and Fibre Channel LEDs

Table 37 describes the LEDs provided during Ethernet, IP, TCP/UDP, and Fibre Channel testing. Only the LEDs that are applicable for your test appear in the LED panel. For example, layer 2 Ethernet, layer 3 IP, and
layer 4 TCP/UDP LEDs do not appear if you configure your unit for a Layer 1 test.

If the instrument loses any of the LED events, the green Status LED extinguishes, and the red Alarm LED in the history column illuminates indicating an error condition has occurred.

Table 37 describes the LEDs, and indicates whether each LED is applicable when testing Ethernet, IP, and Fibre Channel.

Table 37 Ethernet, IP, TCP/UDP, and Fibre Channel LEDs

LED	Indicates	Ethernet	MiM	IP	TCP/UDP	Fibre Channel
Acterna Detect	Green – A frame with an Acterna payload has been detected. Red – An Acterna payload was detected, and then not present for ≥1 second.	√	√			√
ATP Frame Sync	Green – Synchronization with a received ATP frame has been achieved. Red – Synchronization has been lost since the last test restart.					
Frame Detect	Green – Valid frames have been detected. Red – Frames were detected, and then not present for ≥1 second.	√	√	√	√	√
HI-BER	Red (Status) – High Bit Error Rate alarm is currently being detected Red (History) – High Bit Error Rate alarm was detected at some point since the last restart of the test.	10G, 40G & 100G only				

Table 37 Ethernet, IP, TCP/UDP, and Fibre Channel LEDs (Continued)

LED	Indicates	Ethernet	MiM	IP	TCP/UDP	Fibre Channel
IP Packet Detect	Green – An IP Packet has been detected. Red – An IP Packet was detected, and then not present for ≥1 second.			√	√	
LOA (Deskew)	Red – Loss of Alignment (LOA) has occurred between lanes. Red – Loss of Alignment (LOA) has occurred between lanes at some point since the last restart of the test.	40G & 100G only[Γ]				
LOAML	Red – Loss of Alignment Marker Lock (LOAML) has occurred between lanes. Red – Loss of Alignment Marker Lock (LOAML) has occurred between lanes at some point since the last restart of the test.	40G & 100G only[Γ]				
LOBL	Red – Loss of Block Lock (LOBL) has occurred between lanes. Red – Loss of Block Lock (LOBL) has occurred between lanes at some point since the last restart of the test.	40G & 100G only[Γ]				
LPAC	Red – A valid frame was not received within 10 seconds of the last test start or restart.					
L1 Pattern Sync	Green – Synchronization with the received Layer 1 patterns has been achieved. Red – Synchronization has been lost since the last test restart.	√				√
L2 Pattern Sync	Green – Synchronization with the received Layer 2 patterns has been achieved. Red – Synchronization has been lost since the last test restart.	√	√			√

Table 37 Ethernet, IP, TCP/UDP, and Fibre Channel LEDs (Continued)

LED	Indicates	Ethernet	MiM	IP	TCP/UDP	Fibre Channel
Link Active	Green – Auto-negotiation was successful, and link is established with the instrument's link partner. Red – A link to the instrument's link partner has been lost since the last test restart.	√	√	√	√	√
Local Fault Detect	Red (Status) – No local faults are currently being detected. Red (History) – A local fault occurred since the last test restart.	10G, 40G & 100G only				
Marker Lock	Green – (Alignment) Marker Lock has been achieved across all lanes. Red – Alignment Marker Lock was lost on some lane since the las test restart.	40G & 100G only				
Pause Frame Detect	Green – Pause frames have been detected. Red – Pause frames were detected, and then were not present for ≥1 second.	√		√		
PBB Frame Detect	Green – PBB (MAC-in-MAC) frames have been detected. Red – PBB frames were detected, and then were not present for ≥1 second.		√			
Remote Fault Detect	Red – No remote faults are currently being detected. Red – A lremote fault has occurred since the last test restart.	10G, 40G & 100G only				
Signal Present[a]	Green – A signal is present. Red – Received signal has been lost since the last test start or restart.	√	√	√	√	√

Table 37 Ethernet, IP, TCP/UDP, and Fibre Channel LEDs (Continued)

LED	Indicates	Ethernet	MiM	IP	TCP/UDP	Fibre Channel
Status	Green – N/A Red – An error has been recorded by the instrument, as shown in a red Summary Status window.	√	√	√	√	√
SVLAN Frame Detect	Green – SVLAN tagged Ethernet frames have been detected. Red – SVLAN tagged Ethernet frames were detected, and then not present for ≥1 second.	√		√	√	
Sync Acquired	Green – Synchronization is established. Red – Synchronization has been lost since the last test restart.	√	√	√	√	√
TCP Packet Detect	Green – TCP packets have been detected. Red – TCP packets were detected, and then not present for ≥1 second.				√	
UDP Packet Detect	Green – UDP packets have been detected. Red – UDP packets were detected, and then not present for ≥1 second.				√	
VLAN Frame Detect	Green – VLAN tagged Ethernet frames have been detected. Red – VLAN tagged Ethernet frames were detected, and then not present for ≥1 second.	√		√	√	
VLAN Stack Frame Detect	Green – VLAN stack tagged Ethernet frames have been detected. Red – VLAN stack tagged Ethernet frames were detected, and then not present for ≥1 second.	√		√	√	

Table 37 Ethernet, IP, TCP/UDP, and Fibre Channel LEDs (Continued)

LED	Indicates	Ethernet	MiM	IP	TCP/UDP	Fibre Channel
CDMA/GPS Sync[b] (OWD Time Source)	Green – The instrument is within a CDMA/GPS network and has obtain synchronization with the CDMA base station/GPS. Red – The instrument obtained synchronization with the CDMA base station/GPS, and then it was not present for ≥1 second.	√				
1PPS Sync[b] (OWD Time Source)	Green – The instrument is receiving the data that is required to synchronize its internal clock with the GPS time received from the 1 PPS signal. After the CDMA/GPS Sync LED illuminates, this LED may take up to fifteen additional seconds to illuminate. Red – The instrument synchronized the clock with the 1PPS signal, and then it was not present for ≥1 second.	√				

a. The Signal Present LED is not applicable when testing 10/100/1000 Ethernet.
b. If your instrument is equipped with the One Way Delay option, these LEDs appear in the LED panel.

Cable Diagnostic results

The Cable Diagnostics screen shows measurements associated with running cable diagnostics on an electrical link.

After running the Cable Diagnostics tool, the screen lists results for one of the following states:

– **Active 10M or 100M link.** If a 10M or 100M link is established, the MDI/MDIX status (see "MDI or MDIX Status result" on page 351) is reported.
– **Active 1G electrical link.** If a 1G electrical link is established, the pair status, polarity, and pair skew for each MDI pair is reported. See "Skew (ns) result" on page 353, "Polarity result" on page 353 and "Skew (ns) result" on page 353.
– **Inactive link.** If the link is inactive, the unit indicates the type of fault and the fault's relative distance from the tester (see "Distance (m) result" on page 353).

Results associated with cable diagnostics are also provided in the L2 Link Stats result category (see "L2 Link Stats results" on page 355).

MDI or MDIX Status result

The MDI/MDIX Status result indicates the resolved wiring (`MDI`, or `MDIX`) of the near end unit's RJ-45 jack. For example, if the far end can not auto-configure its interface, (in other words, the wiring is fixed), this result can help you determine whether a straight through or crossover cable is being used *or* the MDI/MDIX wiring of the far end port.

– You must know the *fixed MDI/MDIX status* of the far end port to determine the type of cable using the near end MDI/MDIX Status result. For example, if you know that the far end port is fixed at MDI, and the near end port detects MDIX, then you can conclude that a straight through cable is used.
– You must know the *cable type used* to determine the MDI/MDIX status of the far end port using the near end MDI/MDIX Status result. For example, if you know you are using a straight through cable, and the near end port detects MDIX, you can conclude that the wiring at the far end port is MDI.

Table 38 illustrates each of the possible resolutions.

Table 38 Transport Module Ethernet MDI/MDIX Resolution

Far end port	Cable	Near end port
MDIX	straight through	MDI
MDI	cross over	MDI
MDI	straight through	MDIX
MDIX	cross over	MDIX

NOTE:
If the speed detected on the line is 1G electrical, the MDI/MDIX Status results are not applicable and therefore *do not appear* on the Cable Diagnostics screen.

Fault Type result

If a link is inactive, and a fault is detected, the instrument indicates the type of fault detected (`Open`, `Short`, or `Unknown`) and the fault's relative distance from the tester within +/- 1 meter.

If you do not connect the cable to a far end device (completing the circuit), you can also use the Open detection feature to measure the length of a cable.

Fault types are defined as follows:

Open—Indicates there is a cut on the pair (or that the cable is not connected to a device at the far end of the circuit), and that the tester has detected an impedance exceeding 333 ohms. The distance from the near end tester to the end of the cable (or the cut) is also provided.

Short—Indicates a positive and negative line on the same pair are touching, and that the tester has detected an impedance less than 33 ohms.

Unknown—Indicates the tester has detected impedance outside of the ranges stated for Open and Short faults, or that the cable is properly terminated into another Ethernet port. *Unknown does not necessarily indicate that a fault was detected.*

NOTE:
If the far end of the cable is connected to a powered down IP phone, and the phone is an older model, there is a filter that connects between pairs 1-2 and 3-6 in the phone. Depending on the characteristics of the filter, your tester may report a fault for pairs 1-2 and 3-6.

Distance (m) result

For each fault detected, the distance from the Dual Module Carrier, Transport Module, and MSAM to the fault is listed. If no fault is detected, N/A appears.

Skew (ns) result

The Skew result is a measurement of timing differences between the MDI pairs on active 1G electrical links. Timing differences may occur for a variety of reasons. For example, if different insulating materials are used on the pairs, a variance in the signal velocity (skew) may occur. If the skew is significant, transmission of the signal may be impaired to such a degree that the received signal can not be synchronized.

Pair skew is reported in +/- 8 ns increments.

Polarity result

The Polarity result indicates the polarity of each MDI pair on active 1G electrical links, indicating how each pair is physically wired to the unit's port.

– `Normal (+)` indicates a normal polarity for the pair.
– `Inverted (-)` indicates an inverted polarity for the pair.

Pair result

The Pair results for 1G electrical links provide the *current pair assignments for the link*. MDI pairs for 1G electrical links are assigned during the process of auto-negotiation; therefore, if for any reason the link becomes inactive, and then the link is re-established, the pair assignments could potentially change. For example, the first time you establish a link after auto-negotiation, the following pairs could be assigned:

Table 39 MDI pair assignments

MDI0	MDI1	MDI2	MDI3
1-2	3-6	4-5	7-8

If the link goes down (becomes inactive), and then is re-established, the following pairs could be assigned:

Table 40 MDIX pair assignments

MDI0	MDI1	MDI2	MDI3
3-6	1-2	7-8	4-5

SLA/KPI

The Summary SLA/KPI results provide the results relevant to the Service Level Agreement (SLA) and Key Performance Indicators (KPI).

Interface results

Table 41 describes the Interface/Signal results.\

Table 41 Interface/Signal results

Test Result	Description
Link Loss Seconds	Number of seconds during which the link was down (lost).
Local Fault Seconds	Displays the number of test seconds during which a local fault occurred, indicating that the Transport Module could not detect a received signal, could not obtain PCS block synchronization, or detects 16 or more errored PCS block sync headers in a 125 µs period. Only applicable when testing 10 Gigabit Ethernet interfaces.
Optical Rx Level (dBm)	Displays the receive level in dBm when testing optical interfaces using average power consumption (sum of all lanes).
Optical Rx Overload	Displays ON if the received optical power level is greater than the receiver shutdown specification as stated in the specifications appendix of the Getting Started guide that shipped with your instrument, or as stated in the vendor specifications for the transceiver (SFP, XFP, QSFP+ or CFP) you have inserted.
Remote Fault Seconds	Displays the number of test seconds during which the instrument transmits a remote fault indication in response to the receipt of a remote fault indication from its link partner. Only applicable when testing 10 Gigabit, 40 Gigabit, and 100 Gigabit Ethernet interfaces.
Rx Frequency (Hz)	Frequency of the clock recovered from the received signal, expressed in Hz.
Rx Freq Deviation (ppm)	Current received frequency deviation. Displayed in PPM.
Rx Freq Max Deviation (ppm)	Maximum received frequency deviation.
Signal Losses	Number of times signal was lost during current test.
Signal Loss Seconds	Number of seconds during which a signal was not present.
Sync Loss Seconds	Number of seconds during which a synchronization was not present.
Tx Clock Source	Shows the source of the transmit timing standard
Tx Frequency (Hz)	Current transmitter clock frequency, expressed in Hz.
Tx Freq Deviation (ppm)	Current transmitted frequency deviation. Displayed in PPM.
Tx Freq Max Deviation (ppm)	Maximum transmitted frequency deviation.
Wavelength	Displays the current wavelength of the SFP in use.

Table 42 describes the Interface/Lambda results.

Table 42 Interface/Lambda Results (40G/100G applications only)

Test Result	Description
Optical Rx Level (dBm)	Displays the receive level in dBm of each lane when testing some optical interfaces.
QSFP/CFP Per Lane Signal Present	Verifies the presence of an active signal in each lane. Designation of Not Ready indicates presence of device in unit in powered down condition.

Table 42 Interface/Lambda Results (40G/100G applications only)

Test Result	Description
QSFP/CFP Rx Level per Lambda (dbm)	Displays the individual power for each lane and total optical power received in all lanes.
QSFP/CFP Tx Level per Lambda (dbm	Displays the individual power for each lane and total optical power transmitted in all lanes.

L2 Link Stats results

Table 43 describes the L2 Link Stats and L2 Customer Link Stats results such as the average frame rate, peak frame rate, and the maximum, minimum, and average round trip delay measurements. Only results that are applicable to your test appear in the category. For example, the MPLS results only appear when your unit is configured to test using layer 3, MPLS encapsulated traffic. If your unit is configured for a Layer 2 test, MPLS results will not appear.

When testing VPLS or MPLS-TP encapsulated traffic, link statistic results appear in the L2 Customer Link Stats and the L2 SP Link Stats categories.

When testing MiM encapsulated traffic, link statistic results appear in the L2 Customer Link Stats and the L2 Backbone Link Stats categories.

Table 43 L2 Link Stats results

Test Result	Description
B-Tag	Displays the following for the last received backbone frame: Value – Displays the value carried in the B-Tag field (VLAN ID + Priority + Drop Eligible) in a hexa-decimal format. VLAN ID – Displays the ID for the backbone VLAN used as the path to the destination carried in the frame. Priority – Displays the VLAN priority carried in the frame. DEI – Displays the drop eligible bit carried in the frame.
Current Util, %	The current bandwidth utilized by received Broadcast, Unicast, or Multicast traffic expressed as a percentage of the line rate of available bandwidth. This measurement is an average taken over the prior second of test time.

Table 43 L2 Link Stats results (Continued)

Test Result	Description
Delay (μs), Round Trip	You must originate an Acterna payload to measure round trip delay. If a unit is in loopback mode, or if the far end unit is not looped back, invalid results appear because the unit is not originating the traffic. Before measuring delay on 10 Gigabit Ethernet or 10 Gigabit Fibre Channel circuits, you can indicate whether or not you want to make the measurement using a high or low degree of precision. If your delay results say “Out of Range”, change your setting to low precision, and then restart the measurement. Average The average round trip delay calculated in microseconds, with a resolution as follows: – 10/100/1000 and 1 GigE Ethernet: 2.048 μs (ATPv2), 10ns (ATPv3- 1GigE) – 10 Gigabit Ethernet: 2.048 μs (ATPv2), 10ns (ATPv3) – 1G/2G/4Gigabit Fibre Channel: 2.409 μs – 10 Gigabit Fibre Channel: 2.008 μs – 40 Gigabit Ethernet 10ns (ATPv3) – 100 Gigabit Ethernet 10ns (ATPv3) Current – The current round trip delay calculated in microseconds. Maximum – The maximum round trip delay calculated in microseconds. Minimum – The minimum round trip delay calculated in microseconds.
Frame Rate	Current – The current rate of received frames taken over the prior second of test time. Average – The average rate is calculated over the time period elapsed since the last test restart. Minimum – The minimum rate is taken over a one second period. Peak – The maximum rate is taken over a one second period since frame detection. All rates are expressed in *frames per second*.
Frame Size	The average, maximum, and minimum size of frames received since frame detection.
I-Tag	Displays the following for the last received backbone frame: Value – Displays the value carried in the I-Tag field (Service ID + Priority + DEI + Use Customer Address) in a hexadecimal format. Service ID – Displays the service ID carried in the last frame. Priority – Displays the priority carried in the last frame. DEI – Displays the drop eligible bit carried in the last frame. Use Customer Address – Displays the use customer address bit carried in the last frame.
MPLS Label Depth Max	Displays the maximum number of MPLS labels for all frames received since starting the test.
MPLS Label Depth Min	Displays the minimum number of MPLS labels for all frames received since starting the test.
MPLS1 ID	Displays label 1 of the last received MPLS encapsulated frame.
MPLS1 Priority	Displays the label 1 priority of the last received MPLS encapsulated frame.

Table 43 L2 Link Stats results (Continued)

Test Result	Description
MPLS1 TTL	Displays the label 1 TTL value for the last received MPLS encapsulated frame.
MPLS2 ID	Displays label 2 of the last received MPLS encapsulated frame.
MPLS2 Priority	Displays the label 2 priority of the last received MPLS encapsulated frame.
MPLS2 TTL	Displays the label 2 TTL value for the last received MPLS encapsulated frame.
MPLS-TP Label Depth Max	Displays the maximum number of MPLS-TP labels for all frames received since starting the test. *Result appears in the L2 SP Link Stats category.*
MPLS-TP Label Depth Mim	Displays the minimum number of MPLS-TP labels for all frames received since starting the test. *Result appears in the L2 SP Link Stats category.*
MPLS-TP Tunnel Label	Displays the tunnel label of the last MPLS-TP encapsulated frame.
MPLS-TP Tunnel Priority	Displays the tunnel priority of the last MPLS-TP encapsulated frame.
MPLS-TP Tunnel TTL	Displays the tunnel TTL value of the last MPLS-TP encapsulated frame.
MPLS-TP VC Label	Displays the VC label of the last MPLS-TP encapsulated frame.
MPLS-TP VC Priority	Displays the VC priority of the last MPLS-TP encapsulated frame.
MPLS-TP VC TTL	Displays the VC TTL value of the last MPLS-TP encapsulated frame.
One Way Delay (µs)	Average The average one way delay calculated in microseconds, with a resolution as follows: – 10/100/1000 and 1 GigE Ethernet: 2.048 µs(ATPv2), 10ns (ATPv3- 1GigE) – 10 Gigabit Ethernet: 2.048 µs (ATPv2), 10ns (ATPv3) – 1G/2G/4Gigabit Fibre Channel: 2.409 µs – 10 Gigabit Fibre Channel: 2.008 µs Current – The current one way delay calculated in microseconds. Maximum – The maximum one way delay calculated in microseconds. Minimum – The minimum one way delay calculated in microseconds.
One Way Delay % Valid	The ratio of packets containing a GPS timestamp to the total number of Acterna Test Packets received.
OWD ATP Frame Count	The number of ATP-GPS frames received since test restart.
Packet Jitter (µs)	Instantaneous – The current Packet Jitter measured over the prior second of test time. Average – The smoothed average value of the packet delay variation since the last test restart (per RFC 1889), calculated in microseconds. Max Average – The maximum Packet Jitter, Avg (µs) measured since the last test restart, calculated in microseconds. Peak – The highest packet delay variation measured since the last test restart, calculated in microseconds.
Preceding SVLANs	Displays the SVLAN ID, priority, and DEI of stacked VLANs.
Rx Mbps, Cur L1	The current bandwidth utilized by the received traffic expressed in L1 megabits per second, including the preamble, start of frame delimiter, and minimum inter-frame gap.

Table 43 L2 Link Stats results (Continued)

Test Result	Description
Rx Mbps/Kbps L1, Average	The average L1 rate of received frames calculated since the last test restart.
Rx Mbps/Kbps L1, Minimum	The minimum current L1 rate of received frames calculated since the last test restart.
Rx Mbps/Kbps L1, Maximum	The maximum current L1 rate of received frames calculated since the last test restart.
Rx Mbps, Cur L2	The current data rate of received frames calculated over the prior second of test time. Data rate is the frame bandwidth, excluding the preamble, start of frame delimiter, and minimum inter-frame gap.
Rx Mbps/Kbps L2, Average	The average data rate of received frames calculated since the last test restart
Rx Mbps/Kbps L2, Minimum	The minimum current data rate of received frames calculated since the last test restart.
Rx Mbps/Kbps L2, Maximum	The maximum current data rate of received frames calculated since the last test restart.
Rx Pause Length (ms)	The duration, in milliseconds of currently received pause frames taken over the prior second of test time, and the minimum and maximum length since starting or restarting the test.
Svc Disruption (µs)	The service disruption time (maximum inter-frame gap) when service switches to a protect line calculated in microseconds. *Result appears in the L2 SP Link Stats category.*
SVLAN Frame DEI	Displays the DEI of the last received tagged frame.
SVLAN ID	Displays the SVLAN ID of the last received tagged frame.
SVLAN User Priority	Displays the SVLAN priority of the last received tagged frame.
Total Util %	Average – The average bandwidth utilized by the received traffic, expressed as a percentage of the line rate of available bandwidth calculated over the time period since the last test restart. Current – The current bandwidth utilized by the received traffic expressed as a percentage of the line rate of available bandwidth. This measurement is an average taken over the prior second of test time. Minimum – The minimum bandwidth utilized by the received traffic since the last test restart expressed as a percentage of the line rate of available bandwidth. Peak – The peak bandwidth utilized by the received traffic since the last test restart expressed as a percentage of the line rate of available bandwidth. **NOTE:** The bandwidth utilization calculations are made on per-second boundaries and may happen in the middle of a large frame, causing the utilization to be reduced.
Tx Mbps, Cur L1	The current bandwidth utilized by the transmitted traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Tx Mbps, Cur L2	The current data rate of transmitted frames calculated over the prior second of test time. Data rate is the frame bandwidth, excluding the preamble, start of frame delimiter, and minimum inter-frame gap.
VLAN ID	Displays the VLAN ID of the last received tagged frame.
VLAN User Priority	Displays the VLAN priority of the last received tagged frame.

Table 43 L2 Link Stats results (Continued)

Test Result	Description
VPLS Label Depth Max	Displays the maximum number of VPLS labels for all frames received since starting the test. *Result appears in the L2 SP Link Stats category.*
VPLS Label Depth Min	Displays the minimum number of VPLS labels for all frames received since starting the test. *Result appears in the L2 SP Link Stats category.*
VPLS Tunnel Label	Displays the tunnel label of the last received VPLS encapsulated frame.
VPLS Tunnel Priority	Displays the tunnel priority of the last received VPLS encapsulated frame.
VPLS Tunnel TTL	Displays the tunnel TTL value of the last received VPLS encapsulated frame.
VPLS VC Label	Displays the VC label of the last received VPLS encapsulated frame.
VPLS VC Priority	Displays the VC priority of the last received VPLS encapsulated frame.
VPLS VC TTL	Displays the VC TTL value of the last received VPLS encapsulated frame.

L2 Link Counts results

Table 44 describes the L2 Link Counts results, such as the number of received frames, number of transmitted frames, and number of unicast, multicast, or broadcast frames. The Received Frames result includes errored frames; all other results count valid frames only.

When testing VPLS or MPLS-TP encapsulated traffic, the link count results appear in the L2 Customer Link Counts and the L2 SP Link Counts categories.

When testing MiM encapsulated traffic, the link count results appear in the L2 Customer Link Counts and the L2 Backbone Link Counts categories.

Table 44 L2 Link Counts results

Test Result	Description
Jumbo Frames	Jumbo/Oversized frames are counted in this category. This includes count of received Ethernet frames with a length greater than: – 1518 bytes (non-tagged frames) – 1522 bytes (VLAN tagged frames) – 1526 bytes (Q-in-Q encapsulated frames)
1024 - 1518/1522/1526	A count of received Customer Ethernet frames between: – 1024 bytes and 1518 bytes – 1024 to 1522 bytes for VLAN-tagged frames – 1024 to 1526 bytes for Q-in-Q encapsulated frames
1024 - < Jumbo Frames	A count of received Ethernet frames between 1024 bytes and less than Jumbo frames
1024-2140 Byte Frames	A count of received Fibre Channel frames with lengths between 1024 and 2140 bytes, inclusive.
128-252 Byte Frames	A count of received Fibre Channel frames with lengths between 128 and 252 bytes, inclusive.
128-255 Byte Frames	A count of received Ethernet frames with lengths between 128 and 255 bytes, inclusive.
256-508 Byte Frames	A count of received Fibre Channel frames with lengths between 256 and 5088 bytes, inclusive.
256-511 Byte Frames	A count of received Ethernet frames with lengths between 256 and 511 bytes, inclusive.

Table 44 L2 Link Counts results (Continued)

Test Result	Description
28-64 Byte Frames	A count of received Fibre Channel frames with lengths between 28 and 64 bytes, inclusive.
512-1020 Byte Frames	A count of received Fibre Channel frames with lengths between 512 and 1020 bytes, inclusive.
512-1023 Byte Frames	A count of received Ethernet frames with lengths between 512 and 1023 bytes, inclusive.
64 Byte Frames	A count of received Ethernet frames with a length of 64 bytes.
65-127 Byte Frames	A count of received Ethernet frames with lengths between 65 and 127 bytes, inclusive.
68-124 Byte Frames	A count of received Fibre Channel frames with lengths between 68 and 124 bytes, inclusive.
Broadcast Frames	The number of Ethernet broadcast frames received since the last test restart.
Class 1 Frames	A count of received Fibre Channel Class 1 frames since the last test start or restart.
Class 2 Frames	A count of received Fibre Channel Class 2 frames since the last test start or restart.
Class 3 Frames	A count of received Fibre Channel Class 3 frames since the last test start or restart.
Class F Frames	A count of received Fibre Channel Class F frames since the last test start or restart.
Customer Tx Frame Bytes	A count of the total number of VPLS customer frame bytes transmitted since the test was started. The count starts at the Destination Address and continues to the Frame Check Sequence. The count does not include the preamble.
Far End B-B Credits	Count of the number of credits communicated by the far end during ELP login.
MPLS-TP Frames	A count of received MPLS-TP frames since the test was started, including errored frames. *Appears in the L2 SP Link Counts category.*
Multicast Frames	The number of Ethernet multicast frames received since the last test restart.
Near-end B-B Credits	Count of the number of credits communicated by the near-end during Implicit login.
Pause Frames	A count of pause frames received from a remote Ethernet device. Pause frames are utilized for flow control and alert the transmitting device that it must reduce the outgoing frame rate or risk a receiver overflow on the far end, resulting in dropped traffic.
Received Frames	A count of frames received since the last test restart, including errored frames.
Rx Acterna Frames	A count of received Acterna frames, including errored frames.
Rx Acterna OWD Frames	The number of ATP-GPS frames received since test restart.
Rx Collisions	A count of the number of times the unit has received a jam signal while it was not transmitting frames. Result only appears for half-duplex 10/100 Ethernet tests.
Rx Frame Bytes	A count of the total number of frame bytes received since the test was started. The count starts at the Destination Address and continues to the Frame Check Sequence. – The count does not include the preamble or start of frame delimiter. – The count does include errored frames.
Rx LBM Frames	A count of the total number of LBM frames received since the last test restart.
Rx LBR Frames	A count of the total number of LBR frames received since the last test restart.
Rx MPLS Frames	A count of received MPLS frames since the test was started, including errored frames.
Rx Q-in-Q Frames	A count of received QinQ frames since the test was started, including errored frames.
Rx R_RDYs	A count of received Fibre Channel Rx_RDY primitives since the last test start or restart.

Table 44 L2 Link Counts results (Continued)

Test Result	Description
Rx Stacked VLAN Frames	A count of received stacked VLAN frames as defined in IEEE 802.p/q since the test was started, including errored frames.
Rx VLAN Frames	A count of received VLAN frames as defined in IEEE 802.p/q since the test was started, including errored frames.
Rx VPLS Frames	A count of received VPLS frames since the test was started, including errored frames. *Appears in the L2 SP Link Counts category.*
Span Tree Frames	A count of received 802.1d spanning tree frames since frame detection after the last test start or restart.
Transmitted Frames	A count of transmitted frames since the last test restart.
Tx Acterna Frames	A count of transmitted Acterna frames since the last test restart.
Tx Avail B-B Credit, Current	A count of the current number of credits the transmitter can use to send frames. Each time a frame is transmitted, the count decreases by one; each time a frame is acknowledged from the far end through an R_RDY, the count increases by one, up to the maximum value established during login.
Tx Collisions	A count of the number of times the unit has transmitted a frame, and then received a jam signal in the time slot for the frame. Result only appears for half duplex 10/100 Ethernet tests.
Tx Frame Bytes	A count of the total number of frame bytes transmitted since the test was started. The count starts at the Destination Address and continues to the Frame Check Sequence. The count does not include the preamble.
Tx Late Collisions	A count of the number of times the unit has transmitted a frame, and then experiences a collision more than 64 byte times after the transmission begins. Result only appears for half-duplex 10/100 Ethernet tests.
Tx LBM Frames	A count of the total number of LBM frames transmitted since the last test restart
Tx R_RDYs	A count of transmitted Fibre Channel Rx_RDY primitives since the last test start or restart.
Unicast Frames	The number of Ethernet unicast frames received since the last test restart.

L2 Filter Stats results

Table 45 describes the L2 Filter Stats and L2 Customer Filter Stats results for filtered traffic such as the average frame rate, peak frame rate, and the maximum, minimum, and average round trip delay measurements.

When testing VPLS or MPLS-TP encapsulated traffic, the Layer 2 filter statistic results appear in the L2 Customer Filter Stats category.

When testing MiM encapsulated traffic, the Layer 2 filter statistic results appear in the L2 Customer Filter Stats and L2 Backbone Filter Stats categories.

Table 45 L2 Filter Stats and L2 Customer Filter Stats

Test Result	Description
B-Tag	Displays the following for the last filtered backbone frame: Value – Displays the value carried in the B-Tag field (VLAN ID + Priority + Drop Eligible) in a hexadecimal format. VLAN ID – Displays the ID for the backbone VLAN used as the path to the destination carried in the frame. Priority – Displays the VLAN priority carried in the frame. DEI – Displays the drop eligible bit carried in the frame.
Delay (µs)	Average The average round trip delay calculated in microseconds, with a resolution as follows: – 10/100/1000 and 1 GigE Ethernet: 2.048 µs – 10 Gigabit Ethernet: 2.048 µs – 1G/2G/4Gigabit Fibre Channel: 2.409 µs – 10 Gigabit Fibre Channel: 2.008 µs Current – The current round trip delay calculated in microseconds. Maximum – The maximum round trip delay calculated in microseconds. Minimum – The minimum round trip delay calculated in microseconds. **NOTE:** You must originate an Acterna payload to measure round trip delay. If a unit is in loop-back mode, or if the far end unit is not looped back, invalid results appear because the unit is not originating the traffic. Before measuring delay on 10 Gigabit Ethernet or 10 Gigabit Fibre Channel circuits, you can indicate whether or not you want to make the measurement using a high or low degree of precision. If your delay results say “Out of Range”, change your setting to low precision, and then restart the measurement.
Frame Rate	Current – The current rate of filtered frames taken over the prior second of test time. Average – The average rate is calculated over the time period that elapsed since the last test restart. Minimum – The minimum rate is taken over a one second period. Peak – The maximum rate is taken over a one second period since frame detection. All rates are expressed in *frames per second*.
Frame Size	The average, maximum, and minimum size of filtered frames since frame detection.

Table 45 L2 Filter Stats and L2 Customer Filter Stats (Continued)

Test Result	Description
I-Tag	Displays the following for the last filtered backbone frame: Value – Displays the value carried in the I-Tag field (Service ID + Priority + DEI + Use Customer Address) in a hexadecimal format. Service ID – Displays the service ID carried in the last frame. Priority – Displays the priority carried in the last frame. DEI – Displays the drop eligible bit carried in the last frame. Use Customer Address – Displays the use customer address bit carried in the last frame.
MPLS1 ID	Displays label 1 of the last filtered MPLS encapsulated frame.
MPLS1 Priority	Displays the label 1 priority of the last filtered MPLS encapsulated frame.
MPLS1 TTL	Displays the label 1 TTL value for the last filtered MPLS encapsulated frame.
MPLS2 ID	Displays label 2 of the last filtered MPLS encapsulated frame.
MPLS2 Priority	Displays the label 2 priority of the last filtered MPLS encapsulated frame.
MPLS2 TTL	Displays the label 2 TTL value for the last filtered MPLS encapsulated frame.
MPLS-TP Tunnel Label	Displays the tunnel label of the last filtered MPLS-TP encapsulated frame.
MPLS-TP Tunnel Priority	Displays the tunnel priority of the last filtered MPLS-TP encapsulated frame.
MPLS-TP Tunnel TTL	Displays the tunnel TTL value of the last filtered MPLS-TP encapsulated frame.
MPLS-TP VC Label	Displays the VC label of the last filtered MPLS-TP encapsulated frame.
MPLS-TP VC Priority	Displays the VC priority of the last filtered MPLS-TP encapsulated frame.
MPLS-TP VC TTL	Displays the VC TTL value of the last filtered MPLS-TP encapsulated frame.
One Way Delay (μs)	Average The average one way delay calculated in microseconds, with a resolution as follows: – 10/100/1000 and 1 GigE Ethernet: 2.048 ms – 10 Gigabit Ethernet: 2.048 ms – 1G/2G/4Gigabit Fibre Channel: 2.409 ms – 10 Gigabit Fibre Channel: 2.008 ms Current – The current one way delay calculated in microseconds. Maximum – The maximum one way delay calculated in microseconds. Minimum – The minimum one way delay calculated in microseconds.
One Way Delay % Valid	The ratio of packets containing a GPS timestamp to the total number of Acterna Test Packets received.
OWD ATP Frame Count	The number of ATP-GPS frames received since test restart.

Table 45 L2 Filter Stats and L2 Customer Filter Stats (Continued)

Test Result	Description
Packet Jitter (µs)	Instantaneous – The current Packet Jitter measured over the prior second of test time. Average – The smoothed average value of the packet delay variation since the last test restart (per RFC 1889), calculated in microseconds. Max Average – The maximum Packet Jitter, Avg (µs) measured since the last test restart, calculated in microseconds. Peak – The highest packet delay variation measured since the last test restart, calculated in microseconds.
Rx Acterna OWD Frames	The number of filtered ATP-GPS frames received since test restart.
Rx Mbps, Cur L1	The current bandwidth utilized by the filtered traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Mbps, Cur L2	The current data rate of filtered frames calculated over the prior second of test time. Data rate is the frame bandwidth, excluding the preamble, start of frame delimiter, and minimum inter-frame gap.
Rx Stacked VLAN Frames	A count of received stacked VLAN frames as defined in IEEE 802.p/q since the test was started, including errored frames.
SVLAN*x* ID, PRI, DEI	Displays the SVLAN ID, priority, and DEI of each VLAN in the stack.
Svc Disruption (µs)	The service disruption time (maximum inter-frame gap) when service switches to a protect line calculated in microseconds.
Total Util %	Average – The average bandwidth utilized by the filtered traffic, expressed as a percentage of the line rate of available bandwidth calculated over the time period since the last test restart. Current – The current bandwidth utilized by the filtered traffic expressed as a percentage of the line rate of available bandwidth. This measurement is an average taken over the prior second of test time. Minimum – The minimum bandwidth utilized by the filtered traffic since the last test restart expressed as a percentage of the line rate of available bandwidth. Peak – The peak bandwidth utilized by the filtered traffic since the last test restart expressed as a percentage of the line rate of available bandwidth. **NOTE:** The bandwidth utilization calculations are made on per-second boundaries and may happen in the middle of a large frame, causing the utilization to be reduced.
VLAN ID	Displays the VLAN ID of the last filtered tagged frame.
VLAN User Priority	Displays the VLAN priority of the last filtered tagged frame.
VPLS Tunnel Label	Displays the tunnel label of the last filtered VPLS encapsulated frame.
VPLS Tunnel Priority	Displays the tunnel priority of the last filtered VPLS encapsulated frame.
VPLS Tunnel TTL	Displays the tunnel TTL value of the last filtered VPLS encapsulated frame.
VPLS VC Label	Displays the VC label of the last filtered VPLS encapsulated frame.
VPLS VC Priority	Displays the VC priority of the last filtered VPLS encapsulated frame.

Table 45 L2 Filter Stats and L2 Customer Filter Stats (Continued)

Test Result	Description
VPLS VC TTL	Displays the VC TTL value of the last filtered VPLS encapsulated frame.

L2 Filter Counts results

Table 46 describes the L2 Filter Counts L2 Customer Filter Counts results for filtered traffic such as the number of received frames and the number of received frames with an Acterna payload. Only valid frames are counted in this category; errored frames are not counted.

When testing VPLS encapsulated traffic, Layer 2 filter count results appear in the L2 Customer Filter Counts category..

Table 46 L2 Filter Counts results

Test Result	Description
>1518/1522 >1518/1526	A count of filtered Ethernet frames with a length greater than: – 1518 bytes (non-tagged frames) – 1522 bytes (VLAN tagged frames) – 1526 bytes (Q-in-Q encapsulated frames) **NOTE:** Jumbo frames are counted in this category.
1024 - 1518/1522 1024 - 1518/1526	A count of filtered Ethernet frames between: – 1024 bytes and 1518 bytes – 1024 to 1522 bytes for VLAN-tagged frames – 1024 to 1526 bytes for Q-in-Q encapsulated frames
1024-2140 Byte Frames	A count of filtered Fibre Channel frames with lengths between 1024 and 2140 bytes, inclusive.
128-252 Byte Frames	A count of filtered Fibre Channel frames with lengths between 128 and 252 bytes, inclusive.
128-255 Byte Frames	A count of filtered Ethernet frames with lengths between 128 and 255 bytes, inclusive.
256-508 Byte Frames	A count of filtered Fibre Channel frames with lengths between 256 and 5088 bytes, inclusive.
256-511 Byte Frames	A count of filtered Ethernet frames with lengths between 256 and 511 bytes, inclusive.
28-64 Byte Frames	A count of filtered Fibre Channel frames with lengths between 28 and 64 bytes, inclusive.
512-1020 Byte Frames	A count of filtered Fibre Channel frames with lengths between 512 and 1020 bytes, inclusive.
512-1023 Byte Frames	A count of filtered Ethernet frames with lengths between 512 and 1023 bytes, inclusive.
64 Byte Frames	A count of filtered Ethernet frames with a length of 64 bytes.
65-127 Byte Frames	A count of filtered Ethernet frames with lengths between 65 and 127 bytes, inclusive.
68-124 Byte Frames	A count of filtered Fibre Channel frames with lengths between 68 and 124 bytes, inclusive.
Broadcast Frames	The number of filtered Ethernet broadcast frames since the last test restart.
Multicast Frames	The number of filtered Ethernet multicast frames received since the last test restart.
Rx Acterna Frames	A count of received Acterna frames, including errored frames.
Rx Acterna OWD Frames	The number of filtered ATP-GPS frames received since test restart.

Table 46 L2 Filter Counts results (Continued)

Test Result	Description
Rx Frame Bytes	A count of the total number of frame bytes received since the test was started. The count starts at the Destination Address and continues to the Frame Check Sequence. – The count does not include the preamble or start of frame delimiter. – The count does include errored frames.
Rx MPLS Frames	A count of filtered MPLS frames since the test was started, including errored frames.
Rx Q-in-Q Frames	A count of filtered Q-in-Q frames since the test was started, including errored frames.
Rx Stacked VLAN Frames	A count of received stacked VLAN frames as defined in IEEE 802.p/q since the test was started, including errored frames.
Rx VLAN Frames	A count of filtered VLAN frames as defined in IEEE 802.p/q since the test was started, including errored frames.
Rx VPLS Frames	A count of filtered VPLS frames since the test was started, including errored frames. *Appears in the L2 SP Link Counts category.*
Span Tree Frames	A count of filtered 802.1d spanning tree frames since frame detection after the last test start or restart.
Tx ATP Frame Count	A count of transmitted ATP frames at Layer 2.
Unicast Frames	The number of filtered Ethernet unicast frames since the last test restart.
Valid Rx Frames	Count of the number of filtered error-free frames since the test was started.

J-Proof (transparency) results

Table 47 describes the Transparency results associated with the loop back of control frames for various protocols. To view the Transparency results, launch the Layer 2 Traffic application, and then run the transparency test (see “Using J-Proof to verify layer 2 transparency” on page 74)..

Table 47 Transparency results

Test Result	Description
Name	Displays the name specified when you configured the test frame.
Tx	A count of the number of test frames for a particular test frame type transmitted by the instrument since the last test start or restart.
Rx	A count of the number of test frames for a particular test frame type received by the instrument since the last test start or restart.

Table 47 Transparency results (Continued)

Test Result	Description
Status	Displays one of the following: – N/A. Indicates that a particular test frame is not configured to be transmitted. – IDLE. Indicates that a particular test frame is in the queue to be transmitted. – In Progress. Indicates that a particular test frame is currently being transmitted, and has not yet encountered an error. – Timeout. Indicates that for a particular test frame a timeout was reached while waiting for a transmitted frame to return; however, all frames were successfully looped back before the end of the test frame's transmission. – Payload Errors. Indicates that for a particular test frame all transmitted frames were successfully looped back, but a received frame contained a payload that was not the same as its transmitted payload. – Header Errors. Indicates that for a particular test frame, all transmitted frames were successfully looped back, but a received frame contained a header that was different from its transmitted header. – Count Mismatch. Indicates that the number of received frames for a particular test frame did not match the number of frames transmitted.

L2 BERT Stats results

Table 48 describes the L2 BERT Stats results typically associated with the transmission of BERT patterns on a Layer 2 (switched) network. In some instances, the instrument may detect BERT patterns while transmitting an Acterna payload (for example, if a device on the far end of the link is transmitting an all ones BERT pattern).

To view the L2 BERT Stats results while BER testing, transmit traffic with a BERT pattern in the payload over a Layer 2 network, and then set a result category to L2 BERT Stats.

When testing VPLS encapsulated traffic, Layer 2 BERT statistic results appear in the L2 Customer BERT Stats category.



NOTE:

To display Layer 2 BERT Stat results, the Dual Module Carrier, Transport Module, and MSAM must receive frames with a BERT pattern matching the pattern specified in the receive settings (see "Specifying Ethernet filter settings" on page 56).

Table 48 L2 BERT Stats results

Test Result	Description
Bit Error Rate	The ratio of pattern bit errors to received pattern bits since initially acquiring frame synchronization. **NOTE:** This ratio is determined using only the bits in the payload of the frame.
Bit Errored Seconds	The number of seconds during which one or more pattern bit errors occurred since initial frame synchronization.
Bit Errors	A count of the number of received bits in a recognized pattern that do not match the expected value since initially acquiring frame synchronization.
Bit Error-Free Seconds	Number of error-free seconds during which error analysis has been performed since initial pattern synchronization.

Table 48 L2 BERT Stats results (Continued)

Test Result	Description
Bit Error-Free Seconds,%	Number of error-free seconds divided by the number of seconds during which error analysis has been performed since initial pattern synchronization, expressed as a percentage.
Pattern Losses	Count of the number of times pattern synchronization was lost since initially acquiring pattern synchronization.
Pattern Loss Seconds	Count of the number of seconds during which pattern synchronization was lost since initially acquiring pattern synchronization.

CDMA Receiver Status results

Table 49 describes the CDMA Receiver Status results used when testing one way delay.

Table 49 CDMA Receiver results

Test Result	Description
Signal Processor State	Displays the state of the signal processor in the Præcis Cf device.
Base Station Pseudo Noise Offset	Displays the PNO code of the base station that the Præcis Cf device is listening to, between 0 and 511.
Automatic Gain Control	Displays automatic gain control DAC byte, between 0 and 255, but typically between 150 and 220.
Carrier Signal to nose Ratio	Displays the signal to noise ratio (SNR) for received CDMA broadcast channel, between 0.0 and 99.9, but typically between 2.5 and 11.0.
Sync Channel Frame Error Rate	Displays the Sync Channel Frame Error Rate.
TCXO Control	Displays the status of TCXO voltage control. If the TCXO voltage control starts falling outside of the typical range, the Præcis Cf device should be returned to the factory.
No Signal Time-Out	Indicates that the Præcis Cf unit was not able to acquire CDMA for one hour while the Time Figure of merit has been 9.
Hardware Failure Detected	Indicates the Præcis Cf device cannot be expected to work properly due to an internal error.
Time Figure of Merit	Indicates the GPS accuracy of the current signal.
Firmware Version	Displays the firmware of the connected CDMA receiver.

CDMA/GPS Receiver Log

The CDMA Receiver Log provides a listing of significant events and messages, such as sync acquired or CDMA loss.

Ethernet OAM Service OAM results

Table 50 describes the Service OAM results, such as the number of RDI seconds, loss of continuity indicator, and the number of transmitted and received CCM frames. Service OAM results are not applicable with 40G/100G High Speed Transport Module.

Table 50 Ethernet OAM Service OAM results

Test Result		Description
CCM	Loss of Continuity	ON indicates that a loss of continuity has occurred.
	Maint. ID	Displays the maintenance association ID configured for the CCM frame received.
	MD Level	Displays the maintenance domain level configured for the CCM frame received.
	Mismerge	ON indicates that CCM frames have been received with the same maintenance domain level specified for transmitted frames, but the received CCM frames carry a different maintenance association ID (MAID).
	Peer MEG End Point ID	Displays the maintenance entity group end point ID for the instrument's peer as configured.
	RDI	Indicates whether or not remote defect indication is ON or OFF.
	RDI Seconds	Count of the number of seconds during which an RDI was declared since starting or restarting the test.
	Total Rx Frames	Count of the number of CCM frames received since the last OAM setting was specified or changed.
	Total Tx Frames	Count of the number of CCM frames transmitted since the last OAM setting was specified or changed.
	Unexpected MEG Level	ON indicates that CCM frames have been received with a maintenance entity group level lower than that specified as the maintenance domain level when you configured the OAM settings for the transmitting instrument.
	Unexpected MEP	ON indicates that a CCM was received from a different maintenance end point than that specified as the instrument's peer MEG End Point.
	Unexpected Period	ON indicates that a CCM was received with the correct maintenance domain level, maintenance association ID, and maintenance end point ID, but with a period value that was not the same as the instrument's CCM rate.
AIS	AIS	Indicates whether AIS is ON or OFF.
	AIS Seconds	Count of the number of seconds during which an AIS was declared since starting or restarting the test.
	Total Rx Frames	Count of the number of frames received since AIS was declared.
	Total Tx Frames	Count of the number of frames transmitted since AIS was declared.
	Unexpected Period	ON indicates that an AIS was received with the correct maintenance domain level, maintenance association ID, and maintenance end point ID, but with a period value that was not the same as the instrument's AIS rate.
LBM	Total Rx LBM Frames	Count of the total number of LBM frame received since the last OAM setting was specified or changed.
	Total Tx LBM Frames	Count of the total number of LBM frames transmitted since the last OAM setting was specified or changed.
	Total Rx LBR Frames	Count of the total number of LBR frames received since the last OAM setting was specified or changed.
	Total Tx LBR Frames	Count of the total number of LBR frames transmitted since the last OAM setting was specified or changed.

Table 50 Ethernet OAM Service OAM results (Continued)

Test Result		Description
LTM	Total Rx LTM Frames	Count of the total number of LTM frame received since the last OAM setting was specified or changed.
	Total Tx LTM Frames	Count of the total number of LTM frames transmitted since the last OAM setting was specified or changed.
	Total Rx LTR Frames	Count of the total number of LTR frames received since the last OAM setting was specified or changed.
	Total Tx LTR Frames	Count of the total number of LTR frames transmitted since the last OAM setting was specified or changed.
CV/FFD	Expected LSR ID	IPv6 ID entered during setup as the address of the expected LSR
	Expected LSP ID	ID entered during setup as the ID of the expected LSP
	Total Rx CV Frames	Count of the total number of CV OAM packets received since the first received FFD
	Total Tx CV Frames	Count of the total number of CV OAM packets sent
	Total Rx FFD Frames	Count of the total number of FFD OAM packets received since the first received FFD
	Total Tx FFD Frames	Count of the total number of FFD OAM packets sent
	Expected Frequency (FFD)	Display of FFD OAM packets Frequency (Tx) as specifed in setup
	dLOCV	Simple Loss of Connectivity Verification due to missing CV or FFD OAM packets with expected TTSI
	dTTSI Mismatch	Trail Termination Source ID mismatch defect due to unexpected or lack of expected TTSI in CV or FFD OAM packets
	dTTSI Mismerge	Trail Termination Source ID mismerge defect due to both unexpected and expected TTSI in CV or FFD OAM packets
	dExcess	Defect due to a rate of receipt of CV or FFD OAM packets in excess of the nominal receipt rate- 1 per second for CV or 20 per second for FFD
BDI	BDI	Status of BD transmit or receive condition. OFF = BDI button in action bar not clicked
	BDI Seconds	Total seconds since receipt of first BDI
	Defect Type	Type of defect received in BDI OAM packets
	Defect Location	Defect location received in BDI OAM packets
	LSP ID	LSP ID from BDI OAM packets received
	LSR ID	LSR ID from BDI OAM packets received
	Total RX Frames	Total number of BDI packets received since the first BDI or FDI packet was received
	Total Tx Frames	Total number of BDI packets sent

Table 50 Ethernet OAM Service OAM results (Continued)

Test Result		Description
FDI	FDI	Status of BDI or FDI transmit or receive condition. OFF = FDI or BDI button in action bar not clicked
	FDI Seconds	Total seconds since receipt of first FDI
	Defect Type	Type of defect received in FDI OAM packets
	Defect Location	Defect location received in FDI OAM packets
	LSP ID	LSP ID from FDI OAM packets received
	LSR ID	LSR ID from FDI OAM packets received
	Total RX Frames	Total number of FDI packets received since the first BDI or FDI packet was received
	Total Tx Frames	Total number of FDI packets sent

Ethernet OAM Service OAM MEP Discovery results

Table 51 describes the Ethernet OAM Service OAM MEP Discovery results, dealing with identification of network OAM elements and some continuity checking parameters.

Table 51 Ethernet OAM Service OAM MEP Discovery results

Test Result	Description
# of MEPs Discovered	Number of unique MEPs currently displayed
MEP ID	Displays configured ID of the MEG Endpoint (MEPin the incoming CCM)
Source MAC Address	Displays MAC address of the source of the incoming CCM
VLAN ID	Displays VLAN ID in the incoming CCM, if present
SVLAN ID	Displays SVLAN ID in the incoming CCM, if present
MD Level	Displays the configured level of the Maintenance Domain (MD) in the incoming CCM
Specify Domain ID	Displays the configured Specify Domain ID in the incoming CCM
MD ID	Displays the configured Maintenance Domain ID in the incoming CCM
MA ID	Displays configured Maintenance Association (MA) Name or Maintenance Entity Group (MEG) Identification
CCM Rate	Displays configured transmission frequency of the incoming CCM
CCM Type	Displays the configured CCM type in the incoming CCM
* Results can be filtered by a specified value under any of these column headings. Enter data in Filter the Display settings under the Results display window. To expand, select the icon in the lower left corner.	

Ethernet OAM L-OAM Modes results

Table 52 describes the L-OAM Modes results, such as the remote and local mode, parser action, and muxer action. The Link OAM State must be On to observe these results.

L-OAM results are not applicable with 40G/100G High Speed Transport Module.

Table 52 Ethernet OAM L-OAM Modes results (Remote and Local Operation)

Test Result	Description
Mode	Displays the current mode (Active or Passive) for the local or remote instrument.
Parser Action	Indicates the local or remote receiver is currently forwarding, looping back, or discarding non-OAM PDUs.
Muxer Action	Indicates the local or remote transmitter is currently forwarding or discarding non-OAM PDUs.
Vendor OUI	Displays the Vendor OUI (Organizationally Unique Identifier) for the local or remote instrument.
Vendor Specific Info	Displays vendor specific information for the local or remote instrument.
Max PDU Size	Displays the maximum PDU (Protocol Data Units) size supported by the local or remote instrument.
Unidirectional	Indicates whether the local or remote instrument advertises that it is capable of sending OAM PDUs when the receive path is non-operational.
Link Events	Indicates whether the local or remote instrument is configured to monitor link events.
Loopback	Indicates whether the local or remote instrument advertises that it provides loopback support.
Variable Retrieval	Indicates whether the local or remote instrument supports sending Variable Response OAM PDUs.
Revision	Displays the current TLV (Type Length Value) revision for the local or remote instrument.
MAC Address	Displays the MAC address for the remote instrument.

Ethernet OAM L-OAM Counts results

Table 53 describes the L-OAM Counts results, such as the number of transmitted and received variable requests, variable responses, and loop back control frames. The Link OAM State must be On to observe these results.

L-OAM results are not applicable with 40G/100G High Speed Transport Module

Table 53 Ethernet OAM L-OAM Counts results

Test Result	Description
Information	A count of Information frames transmitted or received since starting the test.
Event Notification	A count of Event notification frames transmitted or received since starting the test.
Variable Request	A count of variable request frames transmitted or received since starting the test.
Variable Response	A count of Variable Response frames transmitted or received since starting the test.
Loopback Control	A count of Loopback Control frames transmitted or received since starting the test.
Duplicate Event	A count of duplicate Event notification frames transmitted or received since starting the test.
Unsupported	A count of unsupported frames transmitted or received since starting the test.
Organization Specific	A count of Organization Specific frames transmitted or received since starting the test.

Ethernet OAM L-OAM States results

Table 54 describes the L-OAM States results, such as the Discovery state, and Dying Gasp events. The Link OAM State must be On to observe these results

L-OAM results are not applicable with 40G/100G High Speed Transport Module.

Table 54 Ethernet OAM L-OAM States results

Test Result	Description
Discovery	
State	Displays one of the following: – Fault – Active Send Local – Passive Wait – Send Local Remote – Send Any
Local	Displays one of the following: – 0 = Can't complete – 1 = Not completed – 2 = Completed – 3 = Reserved
Remote	Displays one of the following: – 0 = Can't complete – 1 = Not completed – 2 = Completed – 3 = Reserved
Remote Events	
Link Fault	Indicates whether a link fault occurred.
Dying Gasp	Indicates whether an unrecoverable failure has occurred.
Critical	Indicates whether a critical event has occurred.

Ethernet OAM L-OAM Error History results

Table 55 describes the L-OAM Error History results for Symbol Period Events, Frame Events, Frame Period Events, Frame Sec Summary Events. The Link OAM State must be On to observe these results.

L-OAM results are not applicable with 40G/100G High Speed Transport Module

Table 55 Ethernet OAM L-OAM Error History results

Test Result	Description
Remote Timestamp	Displays the time that the last event occurred.
Remote Window	Indicates the duration of the period.
Remote Threshold	Indicates the number of errors that must occur in the window to cause an event.
Remote Errored Frame Sec	A count of the number of errored seconds in the period.
Remote Errored Frames	A count of errored frames since in the period.

Table 55 Ethernet OAM L-OAM Error History results (Continued)

Test Result	Description
Remote Error Running Total	A count of the number of errors since starting the test.
Remote Running Total	A count of the number of events since starting the test.

L3 Link Stats results

Table 56 describes the L3 Link Stats results, such as the average packet rate, peak packet rate, and the maximum, minimum, and average round trip delay measurements.

Table 56 L3 Link Stats results

Test Result	Description
Packet Rate	Average – The average rate of received packets, calculated over the time period elapsed since the last test restart. Current – The current rate of received packets. This measurement is an average taken over the prior second of test time. Minimum – The minimum rate of received packets over a one second period. Peak – The maximum rate of received packets over a one second period. The packet rate is expressed in packets per second.
Packet Size	Average – The average size of packets received since IP packet detection. Minimum – The minimum size of packets received since IP packet detection. Maximum – The maximum size of packets received since IP packet detection.
Rx Mbps, Cur L3	The current bandwidth utilized by the received IP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Total Util %	Average – The average bandwidth utilized by the received IP traffic. This measurement is an average taken over the prior second of test time. Current – The current bandwidth utilized by the received IP traffic. Minimum – The minimum bandwidth utilized by the received IP traffic since the last test restart. Peak – The peak bandwidth utilized by the received IP traffic since the last test restart. Bandwidth utilization is expressed as a percentage of the line rate of available bandwidth. **NOTE:** The bandwidth utilization calculations are made on per-second boundaries and may happen in the middle of a large frame, causing the utilization to be reduced.
Tx Mbps, Cur L3	The current bandwidth utilized by the transmitted IP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.

L3 Link Counts results

Table 57 describes each of the L3 Link Counts results such as the number of received packets, number of transmitted packets, and number of unicast, multicast, or broadcast packets. The Received Packets result includes errored packets; all other results count valid packets only., Check-marks indicate whether the result is provided for IPv4 or IPv6 traffic

Table 57 L3 Link Counts results

Test Result	IPv4	IPv6	Description
>1500 Byte Packets	√	√	A count of Ethernet IP packets with a length greater than 1500 bytes.
1024-1500 Byte Packets	√	√	A count of Ethernet IP packets with lengths between 1024 and 1500 bytes, inclusive.
128-255 Byte Packets	√	√	A count of Ethernet IP packets with lengths between 128 and 255 bytes, inclusive.
20-45 Byte Packets	√	√	A count of Ethernet IP packets with lengths between 20 and 45 bytes, inclusive.
256-511 Byte Packets	√	√	A count of Ethernet IP packets with lengths between 256 and 511 bytes, inclusive.
46-63 Byte Packets	√	√	A count of Ethernet IP packets with lengths between 46 and 63 bytes, inclusive.
512-1023 Byte Packets	√	√	A count of Ethernet IP packets with lengths between 512 and 1023 bytes, inclusive.
64-127 Byte Packets	√	√	A count of Ethernet IP packets with lengths between 64 and 127 bytes, inclusive.
Broadcast Packets	√	√	The number of Ethernet broadcast IP packets received since the last test restart.
Multicast Packets	√	√	The number of Ethernet multicast IP packets received since the last test restart.
Received Packets	√	√	A count of IP packets received since the last test restart, including errored packets.
Rx Router Advertisements		√	A count of received router advertisement messages when running an IPv6 application. This count is not reset when you restart a test; to reset the count you must bring down the link, reestablish the link, and then start the test again.
Transmitted Packets	√	√	A count of IP packets transmitted since the last test restart. This result does not appear when testing in Monitor mode.
Tx Router Solicitations		√	A count of transmitted router solicitation messages when running an IPv6 application. This count is not reset when you restart a test; to reset the count you must bring down the link, reestablish the link, and then start the test again.
Unicast Packets	√	√	The number of Ethernet unicast IP packets received since the last test restart.

L3 Filter Stats results

Table 58 lists the L3 Filter Stats results for filtered traffic such as the average packet rate, peak packet rate, and the maximum, minimum, and average packet sizes. L3 Filter Stats and Filter Counts exclude errored frames.

Table 58 L3 Filter Stats results

Test Result	Description
Packet Rate	Average – The average rate of filtered packets, calculated over the time period elapsed since the last test restart. Current – The current rate of filtered packets. This measurement is an average taken over the prior second of test time. Minimum – The minimum rate of filtered packets over a one second period. Peak – The maximum rate of filtered packets over a one second period. The packet rate is expressed in packets per second.
Packet Size	Average – The average size of filtered packets since IP packet detection. Minimum – The minimum size of filtered packets since IP packet detection. Maximum – The maximum size of filtered packets since IP packet detection.
Rx Mbps, Cur L3	The current bandwidth utilized by filtered IP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Total Util %	Average – The average bandwidth utilized by filtered IP traffic. This measurement is an average taken over the prior second of test time. Current – The current bandwidth utilized by filtered IP traffic. Minimum – The minimum bandwidth utilized by filtered IP traffic since the last test restart. Peak – The peak bandwidth utilized by filtered IP traffic since the last test restart. Bandwidth utilization is expressed as a percentage of the line rate of available bandwidth. **NOTE:** The bandwidth utilization calculations are made on per-second boundaries and may happen in the middle of a large frame, causing the utilization to be reduced.

L3 Filter Counts results

Table 59 describes each of the L3 Filter Counts results for filtered traffic such as the number of received IP packets, and the number of received packets with an Acterna payload.

Table 59 L3 Filter Counts results

Test Result	IPv4	IPv6	Description
>1500 Byte Packets	√	√	A count of filtered Ethernet IP packets with a length greater than 1500 bytes.
1024-1500 Byte Packets	√	√	A count of filtered Ethernet IP packets with lengths between 1024 and 1500 bytes, inclusive.
128-255 Byte Packets	√	√	A count of filtered Ethernet IP packets with lengths between 128 and 255 bytes, inclusive.
20-45 Byte Packets	√	√	A count of filtered Ethernet IP packets with lengths between 20 and 45 bytes, inclusive.
256-511 Byte Packets	√	√	A count of filtered Ethernet IP packets with lengths between 256 and 511 bytes, inclusive.
46-63 Byte Packets	√	√	A count of filtered Ethernet IP packets with lengths between 46 and 63 bytes, inclusive.
512-1023 Byte Packets	√	√	A count of filtered Ethernet IP packets with lengths between 512 and 1023 bytes, inclusive.
64-127 Byte Packets	√	√	A count of filtered Ethernet IP packets with lengths between 64 and 127 bytes, inclusive.
Broadcast Packets	√	√	The number of filtered Ethernet broadcast IP packets received since the last test restart.
Multicast Packets	√	√	The number of filtered Ethernet multicast IP packets received since the last test restart.
Received Packets	√	√	A count of filtered IP packets received since the last test restart, including errored packets.
Unicast Packets	√	√	The number of filtered Ethernet unicast IP packets received since the last test restart.

L3/IP Config Status results

Table 60 describes the L3 Config Status or IP Config Status results associated with the assignment of static IP addresses, or the assignment if IP addresses by a DHCP server.

Table 60 L3/IP Config Status results

Test Result	IPv4	IPv6	Description
Data Mode	√		Indicates whether you are testing in IPoE or PPPoE mode.
Destination IP Address	√	√	Displays the destination IP address as defined for the currently selected port.
Destination MAC Address	√	√	Displays the hardware (MAC) address of either the gateway or the destination host as resolved by ARP for the currently selected port.
IP Gateway	√	√	Displays the Gateway address assigned by the DHCP server for the currently selected port.

Table 60 L3/IP Config Status results (Continued)

Test Result	IPv4	IPv6	Description
IP Subnet Mask	√		Displays the Subnet mask assigned by the DHCP server for the currently selected port.
PPPoE Status	√		Displays one of the following messages that indicate the current status of the PPPoE session: – INACTIVE – PPPOE ACTIVE – PPP ACTIVE – PPPOE UP – USER REQUESTED INACTIVE – PPPOE TIMEOUT – PPPOE FAILED – PPP LCP FAILED – PPP AUTHENTICATION FAILED – PPP IPCP FAILED – PPP UP FAILED – INVALID CONFIG
Source IP Address	√		Displays the IP address assigned by the DHCP server to the currently selected port.
Src Global IP Address		√	Displays the global address assigned to the instrument manually, or during the auto-configuration process for IPv6 connections.
Src Link-Local IP Address		√	Displays the link local address of the instrument if you are running an IPv6 application. DAD (duplicate address detection) must determine that there are no other devices with the link local address before the address appears.
Subnet Prefix Length		√	Displays the subnet prefix length used to generate the required IPv6 global address for the instrument.
Preferred DNS Address	√	√	The address of the preferred DNS server.
Alternate DNS Address	√	√	The address of the alternate DNS server.
Resolved Name	√	√	The resolved hostname. (The domain name associated with the IP address.)

Ping results

Table 61 describes the Ping results associated with the transmission of Ethernet Ping packets.

Table 61 Ping results

Test Result	Description
Delay, Avg (ms)	The round trip delay for all pings sent and successfully received by the Transport Module since the last test restart. Calculated in milliseconds.
Delay, Max (ms)	The maximum round trip delay for the pings sent and successfully received by the Transport Module. Calculated in milliseconds.
Delay, Min (ms)	The minimum round trip delay for the pings sent and successfully received by the Transport Module. Calculated in milliseconds.
DNS Errors	Count of the DNS errors received during the course of trying to ping the host.

Table 61 Ping results (Continued)

Test Result	Description
Lost Pings	Count of Ping requests sent by the Transport Module for which replies were not received within 3 seconds.
Lost Pings, %	The percentage of the total test seconds during which replies were not received within 3 seconds.
Ping Replies Rx	Count of the ping replies received in response to the ping requests sent by the Transport Module.
Ping Replies Tx	Count of the ping replies sent from the Dual Module Carrier, Transport Module, and MSAM.
Ping Requests Rx	Count of the ping requests received by the Transport Module (in other words, requests sent to the Transport Module's IP address) from another Layer 3 device on the network.
Ping Requests Tx	Count of the ping requests sent from the Transport Module.

Traceroute results

Table 62 describes the results associated with the Traceroute application.

Table 62 Traceroute results

Test Result	Description
Delay (ms)	The round trip delay for the packet. Calculated in milliseconds.
Hop	Displays the hop number for each hop the packet takes while crossing the circuit.
IP Address	Displays the destination IP address for the packet.

PCS Error Stats

Table 63 lists and describes each of the test results available in the PCS Error Stats result category.

Table 63 PCS Error Stats

Test Result	Description
Alignment Marker Loss Seconds	Number of seconds during which Alignment Markers were not detected since initial frame synchronization.
Alignment Marker Lock Present	Alignment Marker Lock condition currently being detected.
Alignment Marker Lock History	Alignment Marker Lock condition detected and then lost at some time since initial frame synchronization.
Invalid Alignment Markers	A count of the number of Invalid Alignment Markers since initial frame synchronization.
Invalid Alignment Markers Rate	The ratio of the sum of Invalid Alignment Markers, across all lanes, to the sum of all Alignment Markers, across all lanes, since initial frame synchronization.
Invalid Alignment Marker Seconds	A count of the number of seconds containing at least one Invalid Alignment Marker, any lane, since initial frame synchronization.
BIP-8 AM Bit Errors	A count of the sum of BIP-8 bit errors, across all lanes, since initial frame synchronization.
BIP-8 AM Bit Errors Rate	The ratio of the sum of BIP-8 bit errors, across all lanes, to the total number of Alignment Markers, across all lanes, since initial frame synchronization.

Table 63 PCS Error Stats (Continued)

Test Result	Description
BIP-8 AM Bit Error Seconds	A count of the number of seconds containing at least one BIP-8 AM Bit Error since initial frame synchronization.
BIP-8 AM Block Errors	A count of the sum total of BIP-8 Block Errors across all lanes since initial frame synchronization.
BIP-8 AM Block Errors Rate	The ratio of the sum of BIP-8 block errors, across all lanes, to the total number of Alignment Markers since initial frame synchronization.
BIP-8 AM Block Error Seconds	A count of the number of seconds containing at least one BIP-8 AM Block Error since initial frame synchronization.
Maximum Skew (bits)	The maximum skew (in bits) between lanes that was detected since Alignment Marker Lock.
LOA (Deskew)	Loss of Alignment of the lanes due excessive interlane skew or invalid Alignment Marker data.
Maximum Skew (ns)	The maximum skew (in ns) between lanes that was detected since Alignment Marker Lock.
Current Maximum Skew (bits)	The maximum inter-lane skew (in bits) that was detected during the period specified for error insertion.
Current Maximum Skew (ns)	The maximum inter-lane skew (in ns) that was detected during the period specified for error insertion.
HI BER Seconds	A count of the number of seconds where High Bit Error Rate (HI BER) was detected in the Sync Bits since initial frame synchronization.
HI BER Present	A High Bit Error Rate (HI BER) was detected in the the Sync Bits since initial frame synchronization.
HI BER History	A High Bit Error Rate (HI BER) was detected in the the Sync Bits at some time in the past after initial frame synchronization.
PCS Block Errors	A count of the number of PCS Block Errors since initial frame synchronization.
PCS Block Error Rate	The ratio of the sum of block errors to the total number of blocks since initial frame synchronization.
PCS Block Error Seconds	A count of the number of seconds containing at least one PCS Block Error since initial frame synchronization.

Ethernet Per Lane results

Table 64 lists and describes each of the test results shown in the Ethernet Per Lane display when performing Ethernet testing. These results appear in a different category depending on the application: for single stream apps, they appear in the Ethernet category, in the multiple stream app, they appear under the link category.

Table 64 Ethernet Per Lane results

Test Result	Description
Max Skew VL ID	Shows Virtual Lane ID for virtual lane having the greatest skew.
Min Skew VL ID	Shows Virtual Lane ID for virtual lane having the least skew.
Max Skew (ns)	Shows skew value in nsecs for virtual lane having the greatest skew.
Max Skew (bits)	Shows skew value in bits for virtual lane having the greatest skew.
Lane #	Shows the virtual Lanes in the signal:40G- #0 - #3, 100G- #0 -#19.

Table 64 Ethernet Per Lane results (Continued)

Test Result	Description
Virtual Lane ID	Shows Lane ID for each virtual lane.
Skew (bits)	Shows skew value in bits for each virtual lane.
Skew (ns)	Shows skew value in nsecs for each virtual lane.
Sync Acquired	Display of sync acquisition status for each virtual lane.
Marker Lock	Display of marker lock status for each virtual lane.
Code Violations	Count of number of code violations for each virtual lane.
Invalid Alignment Markers	Count of the number of invalid alignment markers for each virtual lane.
BIP-8 AM Bit Errors	Count of number of BIP-8 AM Bit errors for each virtual lane.
BIP-8 AM Block Errors	Count of number of BIP-8 AM Block errors for each virtual lane since the start of the test.

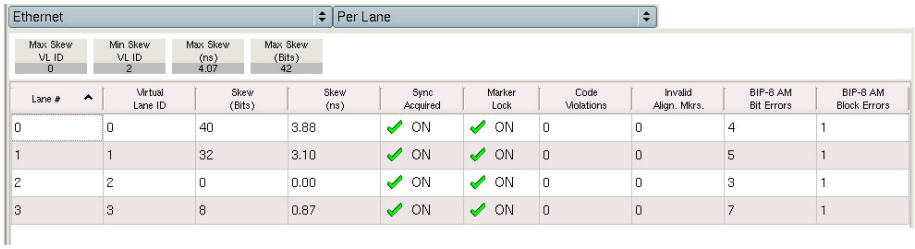


Figure 120 Ethernet Per Lane Results Table

Error Stats results

The Error Stats category lists error statistics such as the number of bit errors, FCS or CRC errored frames, jabbers, runts, and code violations for the Layer 1 BERT, and Layer 2 traffic test applications.

Error Stats (Layer 1 BERT)

Table 65 describes the test results for the Layer 1 BERT patterns.

Table 65 Error Stats results (B Seed, A Seed, and PRBS31 patterns)

Test Result	Description	Pattern 1- B Seed	Pattern 2- A Seed	Pattern 3 - PRBS31	Delay
Bit Error Rate	The ratio of pattern bit errors to received pattern bits since initially acquiring pattern synchronization.			√	
Bit Errors	A count of the number of received bits in a recognized pattern that do not match the expected value.			√	
Code Violation Rate	The ratio of code violations to bits received since the last test restart.	√	√		
Code Violation Seconds	A count of the number of seconds during which code violations occurred.	√	√		

Table 65 Error Stats results (B Seed, A Seed, and PRBS31 patterns) (Continued)

Test Result	Description	Pattern 1- B Seed	Pattern 2- A Seed	Pattern 3 - PRBS31	Delay
Code Violations	A count of each invalid 66-bit code word in the bit stream due to synchronization header errors. For 10GigE and 10G Fibre Channel streams, code words with PCS block errors are also counted as code violations.	√	√		
Error- Free Seconds,%	The percentage of seconds that the received pattern is error free.			√	
Errored Seconds	A count of the number of seconds that the received pattern contained at least one error.			√	
Error-Free Seconds	A count of the number of seconds the pattern is received without any errors.			√	
Pattern Errors	A count of the number of received patterns that do not match the expected pattern.	√	√		
Pattern Error Rate	The ratio of pattern errors to received patterns since initially acquiring pattern synchronization.	√	√		
Pattern Error- Free Seconds, %	The percentage of seconds that the received pattern is error free.	√	√		
Pattern Errored Seconds	A count of the number of seconds that the received pattern contained at least one error.	√	√		
Pattern Error-Free Seconds	A count of the number of seconds the pattern is received without any errors.	√	√		
Pattern Loss Seconds	A count of the number of seconds during which pattern synchronization is lost.	√	√	√	
Total Bits Received	A count of the total number of bits received since the last test restart.			√	
Pattern Sync Losses	Count of the number of times pattern synchronization was lost since initially acquiring pattern synchronization.				√
Pattern Sync Loss Seconds	Count of the number of seconds during which pattern synchronization was lost since initially acquiring pattern synchronization.				√
Round Trip Delay, Current	The current round trip delay calculated in microseconds. This measurement is an average taken over the prior second of time.				√
Round Trip Delay, Average	The average round trip delay measured since starting the test, calculated in microseconds.				√

Table 65 Error Stats results (B Seed, A Seed, and PRBS31 patterns) (Continued)

Test Result	Description	Pattern 1- B Seed	Pattern 2- A Seed	Pattern 3 - PRBS31	Delay
Round Trip Delay, Minimum	The minimum round trip delay measured since starting the test, calculated in microseconds.				√
Round Trip Delay, Maximum	The maximum round trip delay measured since starting the test, calculated in microseconds.				√

Error Stats (Layer 2 Traffic)

For Layer 2 Ethernet and Fibre Channel test applications, to view the Layer 2 Error Stats results described in Table 66, set the result category to Error Stats.

Table 66 Error Stats results (Layer 2 traffic)

Test Result	Description
Alignment Errors	A count of the number of frames received containing both a framing error and an FCS error. Only applicable when testing on 10/100 Mbps circuits.
Alignment Marker Loss Seconds	A count of the seconds since the last valid alignment marker.
Block Sync Losses (PCS)	Count of the number of instances when block synchronization was lost since the last test start or restart. *Only applicable when running 10 GigE applications.*
Code Violation Rate	The ratio of code violations to bits received since the last test restart.
Code Violation Seconds	A count of the number of seconds during which code violations occurred.
Code Violations	A count of each invalid 66-bit code word in the bit stream due to synchronization header errors. For 10GigE and 10G Fibre Channel streams, code words with PCS block errors are also counted as code violations.
CRC Errored Frames	A summed count of Fibre Channel frames containing Cyclic Redundancy Check (CRC) errors. When receiving Fibre Channel jumbo frames containing CRC errors, the CRC error count does not increment. Instead, these frames are counted as Fibre Jabbers.
Errored Blocks (PCS)	Count of the errored blocks received since the last test start or restart. *Only applicable when running 10 GigE applications.*
Errored Frames	– For Ethernet, a summed count of FCS Errored Frames, Jabbers, and Undersized Frames. – For Fibre Channel, a summed count of CRC Errored Frames, Fibre Jabbers, and Undersized Frames.
FCS Errored Frames	A count of Ethernet frames containing Frame Check Sequence (FCS) errors. When receiving Ethernet jumbo frames containing FCS errors, the FCS error count does not increment. Instead, these frames are counted as Jabbers.
Fibre Jabbers	A count of Fibre Channel frames that have a byte value greater than the maximum 2140 frame length and an errored CRC.
Fibre Runts	A count of Fibre Channel frames under the minimum 28 byte frame length containing CRC errors.
Frame Loss Ratio	The ratio of frames lost to the number of frames expected.
Invalid Alignment Markers	A count of the number of alignment markers lost.

Table 66 Error Stats results (Layer 2 traffic) (Continued)

Test Result	Description
Invalid Alignment Marker Rate	A ratio of the number of alignment marks lost to the total number of markers.
Invalid Alignment Marker Seconds	A count of the seconds in which there was at least one invalid alignment marker.
Jabbers	A count of received Ethernet frames that have a byte value greater than the maximum 1518 frame length (or 1522 bytes for VLAN tagged frames or 1526 bytes for Q-in-Q encapsulated frames) and an errored FCS.
Lost Frames	A count of lost Acterna test frames in the traffic. For example, if the Dual Module Carrier, Transport Module, and MSAM detects sequence numbers: 1, 2, 3, 6, 7, 8, (frames 4 and 5 were not detected), the lost frame count is incremented by two (frames 4 and 5 are lost). If the Dual Module Carrier, Transport Module, and MSAM then detects sequence numbers 9, 10, 14, 15, 16 (frames 11, 12, and 13 are missing), the lost frame count is incremented by three, resulting in a total count of five lost frames. **NOTE:** If the Dual Module Carrier, Transport Module, and MSAM receives frames containing errors in the sequence number field, the Lost Frames count may be incorrect.
OoS frames	A count of each instance where the Dual Module Carrier, Transport Module, and MSAM detects out of sequence Acterna test frames in the filtered traffic. For example, if the Dual Module Carrier, Transport Module, and MSAM detects sequence numbers: 1, 2, 3, 6, 7, 8, (frame 6 is detected immediately following frame 3), the out of sequence count is incremented by one, resulting in a count of one instance of out of sequence frames. If the Dual Module Carrier, Transport Module, and MSAM then detects sequence numbers 9, 10, 14, 15, 16 (frame 14 is detected immediately following frame 10), the out of sequence number is incremented again by one, resulting in a total count of two instances of out of sequence frames.
Runts/Undersized	A count of Ethernet frames under the minimum 64 byte frame length.
Symbol Errors	A count of 1 Gigabit Ethernet, 1 Gigabit/2 Gigabit Fibre Channel receive frames with at least one code violation.

Error Stats (Layer 3 Traffic)

For layer 3 test applications, to view the layer 3 Error Stats results described in Table 67, set the result category to Error Stats.

Table 67 Error Stats results (layer 3 traffic)

Test Result	Description
Acterna Payload Errors	A count of received IP packets containing Acterna Payload checksum errors. **NOTE:** This result only appears if you receive an Acterna payload.
Code Violation Rate	The ratio of code violations to bits received since the last test restart.
Code Violation Seconds	A count of the number of seconds during which code violations occurred.
Code Violations	A count of each invalid 66-bit code word in the bit stream due to synchronization header errors. For 10GigE and 10G Fibre Channel streams, code words with PCS block errors are also counted as code violations.
Errored Frames	A summed count of FCS Errored Frames, Jabbers, and Undersized Frames.
Errored Second	The number of available seconds during which one or more relevant errors were present.
Errored Second Ratio	The ratio of errored seconds to the number of available seconds.

Table 67 Error Stats results (layer 3 traffic) (Continued)

Test Result	Description
FCS Errored Frames	A count of Ethernet frames containing Frame Check Sequence (FCS) errors. When receiving Ethernet jumbo frames containing FCS errors, the FCS error count does not increment. Instead, these frames are counted as Jabbers.
Frame Loss Ratio	The ratio of frames lost to the number of frames expected.
IP Checksum Errors	A count of received IP packets with a checksum error in the header.
IP Packet Length Errors	A count of received IP packets that exceed the available Ethernet payload field.
Jabbers	A count of received Ethernet frames that have a byte value greater than the maximum 1518 frame length (or 1522 bytes for VLAN tagged frames) and an errored FCS.
Lost Frames	A count of lost Acterna test frames in the traffic. For example, if the Dual Module Carrier, Transport Module, and MSAM detects sequence numbers: 1, 2, 3, 6, 7, 8, (frames 4 and 5 were not detected), the lost frame count is incremented by two (frames 4 and 5 are lost). If the Dual Module Carrier, Transport Module, and MSAM then detects sequence numbers 9, 10, 14, 15, 16 (frames 11, 12, and 13 are missing), the lost frame count is incremented by three, resulting in a total count of five lost frames. **NOTE:** If the Dual Module Carrier, Transport Module, and MSAM receives frames containing errors in the sequence number field, the Lost Frames count will be incorrect.
OoS Frames	A count of each instance where the Dual Module Carrier, Transport Module, and MSAM detects out of sequence Acterna test frames in the filtered traffic. For example, if the Dual Module Carrier, Transport Module, and MSAM detects sequence numbers: 1, 2, 3, 6, 7, 8, (frame 6 is detected immediately following frame 3), the out of sequence count is incremented by one, resulting in a count of one instance of out of sequence frames. If the Dual Module Carrier, Transport Module, and MSAM then detects sequence numbers 9, 10, 14, 15, 16 (frame 14 is detected immediately following frame 10), the out of sequence number is incremented again by one, resulting in a total count of two instances of out of sequence frames.
Packet Error Rate	The ratio of lost packets to the number of total packets.
Runts/Undersized	A count of Ethernet frames under the minimum 64 byte frame length.
Severely Errored Second	Seconds during which 30% or more of the frames were lost, contained FCS errors, or Loss of Link was detected. The following calculation is used to declare an SES: (FCS Error count + Lost Frame count) / (Frames Received count + Lost Frames) $\geq$ 0.3.
Severely Errored Second Ratio	The ratio of severely errored seconds to the number of available seconds.
Symbol Errors	A count of 1 Gigabit Ethernet, 1 Gigabit/2 Gigabit Fibre Channel receive frames with at least one code violation.
Unavailable Second	Unavailable time is defined as ten (10) consecutive severely errored seconds. These ten seconds are included in the UAS count. For example, if 12 consecutive SES occur, the UAS count will be 12. If only 3 consecutive SES occur, the UAS count will be zero.

Capture results

If you capture packets to analyze using Wireshark®, the Capture category provides a count of the number of packets processed, and displays a gauge indicating the percent of the buffer that is filled with captured packets.

Sync Status Messages

If you are testing on a SyncE or GigE circuit (except 40GigE or 100GigE), the Sync Status Messages category provides results related to SyncE testing. Table 68 describes the test results for the Layer 1 BERT patterns.

Table 68 Sync Status Messages results

Test Result	Description
Decoded QL Message	Decode of the last quality level (QL) message
SSM Message Count Total	Count of all SSM messages received.
SSM Message Count Event	Count of the SSM Event messages received.
SSM Message Count Information	Count of the SSM Information messages received.
SSM Message Count Malformed	Count of the SSM Malformed messages received.
SSM PDU Rate (pps)	Rate of the PDU (Protocol Data Unit).
Tx SSM Count	Count of all SSM messages sent.

On the Summary results page, the “Wrong SSM PDU Rate” result may appear. This alarm indicates that the PDU rate is slower than 1pps or faster than 10pps.

AutoNeg Status results

The AutoNeg Status category displays results associated with the auto-negotiation of capabilities between two Ethernet devices.

Table 69 describes each of the results for 10/100/1000 links.

NOTE:

AutoNeg Status results only appear when auto-negotiation is turned ON on the CSAM, MSAM, or T-BERD/MTS 5800.

Table 69 AutoNeg Status results

Test Result	Description
1000Base - TX FDX	Indicates that the Ethernet link partner is full duplex capable at 1000Base-TX (YES or NO).
1000Base - TX HDX	Indicates that the Ethernet link partner is half duplex capable 1000Base-TX (YES or NO).
100Base-TX FDX	Indicates whether the Ethernet link partner is full duplex capable at 100Base-TX (YES or NO).
100Base-TX HDX	Indicates whether the Ethernet link partner is half duplex capable at 100Base-TX (YES or NO).
10Base-TX FDX	Indicates whether the Ethernet link partner is full duplex capable at 10Base-TX (YES or NO).
10Base-TX HDX	Indicates whether the Ethernet link partner is half duplex capable at 10Base-TX (YES or NO).
Duplex	Indicates the negotiated duplex setting for the link (half or full).

Table 69 AutoNeg Status results (Continued)

Test Result	Description
Link Advt. Status	Indicates that the Dual Module Carrier, Transport Module, and MSAM has received a valid auto-negotiation capability advertisement from the Ethernet link partner and sent an acknowledgement.
Link Config ACK	Indicates that the Ethernet link partner has acknowledged the receipt of a valid auto-negotiation capability advertisement from the Dual Module Carrier, Transport Module, and MSAM.
Mstr/Slv Resolution	Indicates whether the Ethernet link partner is operating as the master (providing the clock for timing), or slave (deriving the clock from the Dual Module Carrier, Transport Module, and MSAM). Applicable when testing 1000 Base-Tx only.
Remote Fault	If supported by the Ethernet link partner, indicates a reason for auto-negotiation failure. If auto-negotiation succeeded, the result will read “NO”.
Speed (Mbps)	Indicates the negotiated speed setting for the link (10 or 100 Mbps).

Table 70 describes each of the results for 1 Gigabit Ethernet optical links.

Table 70 1 Gigabit Ethernet Optical AutoNeg Status results

Test Result	Description
FDX Capable	Indicates whether the Ethernet link partner is full duplex capable (YES or NO).
Flow Control	Indicates whether Flow Control is turned On or Off on your unit.
HDX Capable	Indicates whether the Ethernet link partner is half duplex capable (YES or NO).
Link Advt. Status	Indicates that the Dual Module Carrier, Transport Module, and MSAM has received a valid auto-negotiation capability advertisement from the Ethernet link partner and sent an acknowledgement.
Link Config ACK	Indicates that the Ethernet link partner has acknowledged the receipt of a valid auto-negotiation capability advertisement from the Dual Module Carrier, Transport Module, and MSAM.
Pause Capable	Indicates the flow control capabilities of the Ethernet link partner. Those capabilities are: – Tx Only: The Ethernet link partner will transmit PAUSE frames to alert the Transport Module to reduce the transmitted bandwidth momentarily, however it will not reduce its transmitted bandwidth if it receives PAUSE frames. – Rx Only: The Ethernet link partner will reduce its transmitted bandwidth momentarily if it receives PAUSE frames but it will not transmit PAUSE frames to alert the Transport Module to reduce the transmitted bandwidth. – Both Rx and Tx: The Ethernet link partner will transmit PAUSE frames to alert the Transport Module to reduce the transmitted bandwidth momentarily and it will reduce its transmitted bandwidth momentarily if it receives PAUSE frames – Neither Rx or Tx: The Ethernet link partner will not transmit PAUSE frames to alert the Transport Module to reduce the transmitted bandwidth and it will not reduce its transmitted bandwidth if it receives PAUSE frames.
Remote Fault	If supported by the Ethernet link partner, indicates a reason for auto-negotiation failure. If auto-negotiation succeeded, the result will read “NO”.

Login Status results

The Login Status category displays results associated with the login status between two Fibre Channel devices.

Implicit or Explicit (E-Port) login

Table 71 describes each of the results when using an Implicit or Explicit (E-Port) login.

Table 71 Login Status results - Implicit or Explicit (E-Port) login

Test Result	Description
Login Status	Indicates the status of the Fibre Channel login process by displaying one of the following: – IN PROGRESS – COMPLETE – FAILED/LOOP
RX ELP Accept	Count of accept messages received in response to login requests.
RX ELP Ack1	Count of acknowledgements received in response to login requests or accept/reject messages.
RX ELP Reject	Count of rejections received in response to login requests.
RX ELP Request	Count of login requests received from another JDSU compliant Ethernet tester or a distance extension device.
TX ELP Accept	Count of accept messages transmitted in response to login requests from another JDSU compliant Ethernet tester or a distance extension device.
TX ELP Ack1	Count of acknowledgements transmitted in response to login requests or accept/reject messages from another JDSU compliant Ethernet tester or a distance extension device.
TX ELP Reject	Count of rejections transmitted in response to login requests from JDSU compliant Ethernet tester or a distance extension device.
TX ELP Request	Count of login requests transmitted to another JDSU compliant Ethernet tester or a distance extension device.

Explicit (Fabric/N-Port) login

Table 72 describes each of the results when using an Implicit or Explicit (E-Port) login.

Table 72 Login Status results - Explicit (Fabric/N-Port) login

Test Result	Description
Fabric Present	Indicates whether a fabric is present (Yes or No).
Fabric Login Status	Indicates the status of the fabric login process by displaying one of the following: – In Progress – Complete – Failed/Loop – Unavailable
F Port Name	Displays the name of the F Port that the instrument logged into.
Fabric Name	Displays the name of the fabric that the instrument logged into.

Table 72 Login Status results - Explicit (Fabric/N-Port) login (Continued)

Test Result	Description
N Port Login Status	Indicates the status of the N Port login process by displaying one of the following: – In Progress – Complete – Failed/Loop – Unavailable
Dest. N Port ID	Displays the port ID for the destination N port.
Dest. N Port Name	Displays the name of the destination N port.
Dest. Node Name	Displays the name of the destination node.
Source N Port ID	Displays the port ID for the source N port.
Source N Port Name	Displays the name of the source N port.
Source Node Name	Displays the name of the source node.

PTP Link Counts results

Table 73 describes the PTP Link Counts results. The results that appear vary depending on whether you are using Master or Slave mode.

Table 73 PTP Link Counts results

Test Result	Description
Domain Mismatches	The count of domain mismatched messages.
Rx Frame Counts, Announce	The count of received announce messages.
Rx Frame Counts, Sync	The count of received sync frames.
Rx Frame Counts, Follow Up	The count of received follow up frames.
Rx Frame Counts, Delay Response	The count of received delay response frames.
Rx Frame Counts, Signaling	The count of received signaling frames.
Rx Frame Counts, Management	The count of received management frames.
Tx Frame Counts, Delay Request	The count of transmitted delay request messages.
Tx Frame Counts, Signaling	The count of transmitted signaling frames.
Tx Frame Counts, Management	The count of received management frames.
Rx Frame Rates, Announce	The rate of received announce messages.
Rx Frame Rates, Sync	The rate of received sync frames.
Rx Frame Rates, Follow Up	The rate of received follow up frames.
Rx Frame Rates, Delay Response	The rate of received delay response frames.
Rx Frame Rates, Signaling	The rate of received signaling frames.
Rx Frame Rates, Management	The rate of received management frames.
Tx Frame Rates, Delay Request	The rate of transmitted delay request messages.
Tx Frame Rates, Signaling	The rate of transmitted signaling frames.
Tx Frame Rates, Management	The rate of transmitted management frames.

PTP Link Stats results

Table 74 describes the PTP Link Stats results. The results that appear vary depending on whether you are using Master or Slave mode.

Table 74 PTP Link Stats results

Test Result	Description
Port State	Reports the state of the PTP port: – INITIALIZING: the port initializes its data sets, hardware, and communication facilities. If one port of a boundary clock is in the INITIALIZING state, then all ports shall be in the INITIALIZING state. – FAULTY: The fault state of the protocol. A port in this state shall not place any PTP messages except for management messages that are a required response to another management message on its communication path. – DISABLED: The port shall not place any messages on its communication path. A port in this state shall discard all PTP received messages except for management messages. – LISTENING: The port is waiting for the announce Receipt Timeout to expire or to receive an Announce message from a master. – PRE_MASTER: The port behaves in all respects as though it were in the MASTER state except that it shall not place any messages on its communication path except for Pdelay_Req, Pdelay_Resp, Pdelay_Resp_Follow_Up, signaling, or management messages. – MASTER: The port is behaving as a master port. – PASSIVE: The port shall not place any messages on its communication path except for Pdelay_Req, Pdelay_Resp, Pdelay_Resp_Follow_Up, or signaling messages, or management messages that are a required response to another management message. – UNCALIBRATED: One or more master ports have been detected in the domain. This is a transient state to allow initialization of synchronization servos, updating of data sets when a new master port has been selected, and other implementation-specific activity. – SLAVE:The port is synchronizing to the selected master port.
Source IP Address	In Slave mode, reports the destination IP of the master.
Unicast Lease Duration	The granted lease duration in seconds.
Grandmaster ID	The unique identifier for the grandmaster clock. This is a 64-bit unique identifier derived from the master's 48 bit MAC address, but it is not the MAC address itself. The formula for computing the expanded ID is: <First three bytes of MAC>:FF:FE:<last three bytes of MAC>.
Grandmaster Clock Class	Displays the traceability of the time or frequency distributed by the grandmaster clock.
Grandmaster Clock Accuracy	Displays the characterization of the grandmaster clock for the purpose of the best grandmaster clock algorithm.
Grandmaster Time Source	Indicates the source of the time used by the grandmaster clock.
Grandmaster Priority 1	Displays the priority 1 value, used in the execution of the best master clock algorithm. Lower values take precedence.
Grandmaster Priority 2	Displays the priority 2 value, used in the execution of the best master clock algorithm. Lower values take precedence.
Master-to-Slave Timestamps Converging	Displays whether master and slave time stamps are getting closer together over time.

Table 74 PTP Link Stats results (Continued)

Test Result	Description
Mean Path Delay Average	Mean Path Delay - mean propagation time between a master and slave as computed by the slave, and is calculated by (Tms-Tsm)/2. It is calculated based on the current Delay Request propagation time (Tsm) and Sync propagation time (Tms) pair. MPD, Average - average value of all MPDs since beginning of test (since last test restart). [MPD(1) + MPD(2) + MPD(3) + …. MPD(N)]/N.
Mean Path Delay Current	MPD, Current - current 1 second value of MPD in this test. MPD[i] where is [i] is the current second.
Mean Path Delay Minimum	MPD, Minimum - smallest value of MPD in this test.
Mean Path Delay Maximum	MPD, Maximum - largest value of MPD in this test.
One-Way Delay (OWD), Master-Slave (µs)	One-way Path Delay, Master to Slave reported in the following categories- – Average – Current – Minimum – Maximum
One-Way Delay (OWD), Slave-Master (µs)	One-way Path Delay, Slave to Master reported in the following categories- – Average – Current – Minimum – Maximum
Offset from Master Average	The average offset from master from test restart.
Offset from Master Current	The current offset from master from test restart.
Offset from Master Minimum	The minimum offset from master from test restart.
Offset from Master Maximum	The maximum offset from master from test restart.
Sync PDV Average	The average variation in Sync packet delay (master to slave) from the minimum Sync packet delay.
Sync PDV Current	The current variation in Sync packet delay (master to slave) from the minimum Sync packet delay.
Sync PDV Minimum	The minimum variation in Sync packet delay (master to slave) from the minimum Sync packet delay.
Sync PDV Maximum	The maximum variation in Sync packet delay (master to slave) from the minimum Sync packet delay.
Delay Request IPDV Average	The average variation in Delay Request packet delay (slave to master) from the minimum Delay Request packet delay.
Delay Request IPDV Current	The current variation in Delay Request packet delay (slave to master) from the minimum Delay Request packet delay.
Delay Request IPDV Minimum	The minimum variation in Delay Request packet delay (slave to master) from the minimum Delay Request packet delay.
Delay Request IPDV Maximum	The maximum variation in Delay Request packet delay (slave to master) from the minimum Delay Request packet delay.

PTP Graphs

The following PTP results are available in graphical form:

- Mean Path Delay — The current and average mean path delay from test restart.
- Offset from Master — The current and average offset from master from test restart.
- Sync PDV — The current and average sync PDV from test restart.
- Delay Request PDV — The current and average delay request PDV from test restart.
- Sync IPDV — The current and average sync IPDV from test restart.
- Delay Request IPDV— The current and average delay request IPDV from test restart.
- Master to Slave, OWD— The current and average One-Way Delay from Master to Slave from test restart.
- Slave to Master, OWD— The current and average One-Way Delay from Slave to Master from test restart.

L4 Link Stats results

Table 75 describes the L4 Link Stats results, such as the source and destination port carried in the last layer 4 packet received, and the current bandwidth utilized by TCP or UDP traffic.

Table 75 L4 Link Stats results

Test Result	Description
Rx Destination Port	Displays the Destination Port number for the last layer 4 packet received.
Rx Mbps, Cur L4	The current bandwidth utilized by the received layer 4 (TCP/UDP) traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Mbps, Cur TCP	The current bandwidth utilized by the received TCP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Mbps, Cur UDP	The current bandwidth utilized by the received UDP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Source Port	Displays the Source Port number for the last layer 4 packet received.
Tx Mbps, Cur L4	The current bandwidth utilized by the transmitted TCP/UDP traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.

Detailed L4 Stats

When running the TCP Wirespeed application, detailed statistics are provided for each established connection, including bandwidth measurements, delay measurements, window statistics, and frame counts. Table 78 describes the Detailed L4 Stats results.

Table 76 Detailed L4 Stats results

Test Result	Description
Estab.	Indicates whether or not a connection was established.
Local Port	Displays the local port number for the connection.
Negotiated MSS	The value of the negotiated Max Segment Size.
Remote Port	Displays the remote port number for the connection.

Table 76 Detailed L4 Stats results (Continued)

Test Result	Description
Rx Mbps, Cur	The current bandwidth utilized by the received traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Rx Mbps, Avg	The average bandwidth utilized by the received traffic since starting the test expressed in megabits per second.
Rx Mbps, Min	The minimum bandwidth utilized by the received traffic since starting the test expressed in megabits per second.
Rx Mbps, Max	The maximum bandwidth utilized by the received traffic since starting the test expressed in megabits per second.
Tx Mbps, Cur	The current bandwidth utilized by the transmitted traffic expressed in megabits per second. This measurement is an average taken over the prior second of test time.
Tx Mbps, Avg	The average bandwidth utilized by the transmitted traffic since starting the test expressed in megabits per second.
Tx Mbps, Min	The minimum bandwidth utilized by the transmitted traffic since starting the test expressed in megabits per second.
Tx Mbps, Max	The maximum bandwidth utilized by the transmitted traffic since starting the test expressed in megabits per second.
Rx Send Wind Clsd Cnt	Count of times the far end window closed as a result of reaching its limit.
Tx Total Retrans Frames	Count of the total number of frames retransmitted.
Send Window, Cur	The current window size. This measurement is an average taken over the prior second of test time.
Send Window, Min	The minimum window size utilized since starting the test.
Send Window, Max	The maximum window size utilized since starting the test.
RTD, Cur (ms)	The current round trip delay calculated in milliseconds. This measurement is an average taken over the prior second of time.
RTD, Avg (ms)	The average round trip delay measured since starting the test, calculated in milliseconds.
RTD, Min (ms)	The minimum round trip delay measured since starting the test, calculated in milliseconds.
RTD, Max (ms)	The maximum round trip delay measured since starting the test, calculated in milliseconds.

Cumulative L4 results

When running the TCP Wirespeed application, cumulative statistics are provided for all connections. Table 78 describes the Cumulative L4 results.

Table 77 Detailed L4 Stats results

Test Result	Description
Total Tx Mbps, Cur.	Sum total of transmit throughput of all the valid connections (up to 64 TCP connections).
Total Rx Mbps, Cur.	Sum total of receive throughput of all the valid connections (up to 64 TCP connections).

Table 77 Detailed L4 Stats results (Continued)

Test Result	Description
Total Tx Retrans Frm	Sum total of Tx re-transmit frame count of all the valid connections (up to 64 TCP connections).
Established Connections	Number of active connections.

L4 Link Counts results

Table 78 describes the L4 Link Counts results.

Table 78 L4 Link Counts results

Test Result	Description
TCP Packets	A count of TCP packets received since the last test start or restart.
UDP Packets	A count of TCP packets received since the last test start or restart.

L4 Filter Stats results

Table 79 describes the L4 Filter Stats result.

Table 79 L4 Filter Stats results

Test Result	Description
Rx Mbps, Cur L4	The current bandwidth utilized by filtered layer 4 (TCP/UDP) traffic expressed in mega-bits per second. This measurement is an average taken over the prior second of test time.

L4 Filter Counts results

Table 80 describes the L4 Filter Counts results.

Table 80 L4 Filter Counts results

Test Result	Description
TCP Packets	A count of filtered TCP packets received since the last test start or restart.
UDP Packets	A count of filtered TCP packets received since the last test start or restart.

J-Profiler results

Table 81 describes the results provided when you run the J-Profiler application.

Table 81 Traffic Profiler Streams results

Test Result	Description
MPLS/MPLS1 Label	Displays the label attached to groups of profiled streams.
MPLS/MPLS1 Priority	Displays the priority of the identified stream.

Table 81 Traffic Profiler Streams results (Continued)

Test Result	Description
MPLS PW/MPLS2 Label	Displays the label attached to groups of profiled streams on a pseudo wire.
MPLS PW/MPLS2 Priority	Displays the priority of the identified stream.
VLAN/SVLAN ID	Displays the ID of the provider VLAN
VLAN/SVLAN Priority	Displays the priority of the identified VLAN.
CVLAN ID	Displays the ID of the customer VLAN.
CVLAN Priority	Displays the priority of the identified VLAN.
Source MAC	Displays the source MAC address for the discovered stream.
Source IP	Displays the source IP address for the discovered stream.
Destination MAC	Displays the destination MAC address for the discovered stream.
Destination IP	Displays the destination IP address for the discovered stream.
Source Port	Displays the source port number for the discovered stream.
Source Port Name	Displays the source port name for the discovered stream.
Dest Port	Displays the destination port number for the discovered stream.
Dest Port Name	Displays the destination port name for the discovered stream.
L1 Mbps	Displays the Layer 1 bandwidth utilized for the discovered stream (in Mbps).
Util %	Displays the current bandwidth utilized by the stream expressed as a percentage of the line rate of available bandwidth. This measurement is an average taken over the prior second of test time.
IP DSCP	Displays the DSCP value for the discovered stream.
Frames	A count of received Ethernet frames for the discovered stream.
Frame Size, Max	The maximum size of frames received for the discovered stream since frame detection.
Frame Size, Min	The minimum size of frames received for the discovered stream since frame detection.
Bytes	A count of received bytes for the discovered stream.

Wander Interface results

When configured for wander tests on a 1GigE Optical interface, wander results are available in the Interface result group. Table 82 lists and describes each of the test results available in the Wander result category.

Table 82 Wander test results

Test Result	Description
TIE	The aggregate variation in time delay of the received signal with respect to the reference since the last test start or restart.
Max. TIE	The maximum aggregated Time Interval Error measured since the last test start or restart.
Min. TIE	The minimum aggregated Time interval error measured since the last test start or restart.
MTIE	The largest peak-to-peak TIE detected since the last test start or restart.

Table 82 Wander test results

Test Result	Description
Max. Wander Time Remaining	Time remaining until Wander memory is filled.
Signal Present	Indicates that the data signal is valid.
Wander Reference Present	Indicates that the reference signal is valid.
Rx Frequency (Hz)	Current frequency of the timing signal being analyzed.
Reference Frequency Deviation (ppm)	Difference between frequency of the timing signal and the reference signal. (TOO HIGH or TOO LOW)

In addition, the Wander Analysis provides the following results:

– MTIE — Maximum Time Interval Error. Per ITU-T O.172, MTIE is a measure of wander that characterizes frequency offsets and phase transients. It is a function of parameter τ called the Observation Interval. MTIE(τ) is the largest peak-to-peak TIE detected since the test started.

– TDEV — Time Deviation. Per ITU-T O.172, TDEV is a measure of wander that characterizes its spectral content. It is also a function of parameter τ (the Observation Interval). TDEV(τ) can be said to be the RMS of filtered TIE, where a band-pass filter is centered on a frequency of 0.42/τ.

– Wander Time Remaining — Shows the remaining time left in the wander test in days, hours, minutes, seconds, based on file size and/or disk space constraints.

For detailed information about MTIE and TDEV analysis, see Principles of Jitter and Wander Testing. in the *PDH_SONET Testing Guide* that shipped with this unit.

When testing wander, you can view results in a graphical format by selecting the Wander Graph result categories in the Interface group (see Figure 121).

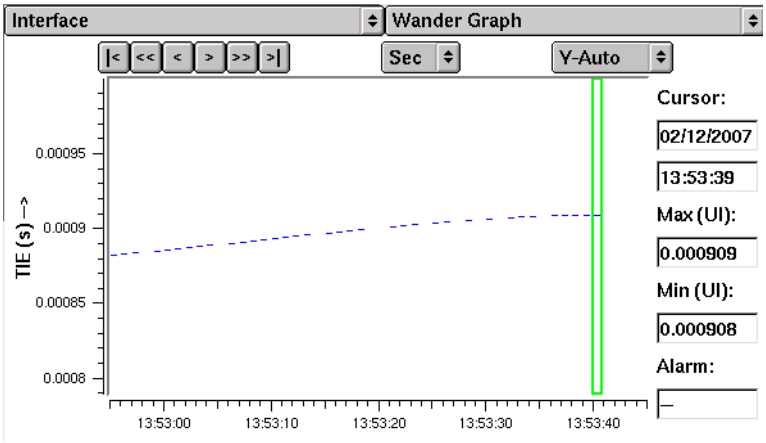


Figure 121 Wander Graph result

IP Video results

Test results that help you evaluate the quality of the physical, link, transport stream, and video stream layers are available when testing IP Video service. A detailed discussion of the layout and principals behind these results is provided in the "Understanding IP Video test results" on page 207 section of Chapter 9 "IP Video Testing".

Categories discussed in this section include the following:

– "IP Video LEDs" on page 398
– "Physical/Link Stats results" on page 399
– "All Streams Transport results" on page 400
– "All Streams Video/All Program Video results" on page 403
– "All Streams Complete results" on page 405
– "Individual stream results" on page 406
– "Stream and Program PID results" on page 406
– "MSTV results" on page 407

IP Video LEDs

Table 83 describes the LEDs provided during IP Video testing. Only the LEDs that are applicable for your test appear in the LED panel.

If the instrument loses any of the LED events, the green Status LED extinguishes, and the red Alarm LED in the history column illuminates indicating an error condition has occurred. For details, refer to "Understanding the LED panel" on page 206 of Chapter 9 "IP Video Testing".

Table 37 describes the LEDs, and indicates whether each LED is applicable when testing IP Video.

Table 83 IP Video LEDs

LED	Indicates
Frame Detect	Green – Valid frames have been detected. Red – Frames were detected, and then not present for ≥ 1 second.
Packet Detect	Green – An IP Packet has been detected. Red – An IP Packet was detected, and then not present for ≥ 1 second.
Link Active	Green – Auto-negotiation was successful, and link is established with the instrument's link partner. Red – A link to the instrument's link partner has been lost since the last test restart.
Signal Present[a]	Green – A signal is present. Red – Received signal has been lost since the last test start or restart.

Table 83 IP Video LEDs (Continued)

LED	Indicates
Sync Acquired	Green – Synchronization is established. Red – Synchronization has been lost since the last test restart.

a. The Signal Present LED is not applicable when testing 10/100/1000 Ethernet.

Physical/Link Stats results

Table 84 lists the results provided in the Physical/Link result group, Stats category.

Table 84 Physical/Link Stats results

Test Result	For Descriptions, Refer to....
Link Active Signal Present Sync Acquired	Table on page 347 (“Ethernet, IP, TCP/UDP, and Fibre Channel LEDs”)
Local Fault Detect Local Fault Seconds Optical Rx Level (dBm) Optical Rx Overload Signal Losses Signal Loss Seconds Link Loss Seconds Sync Loss Seconds	Table on page 354 (“Interface results”)
Code Violations Errored Frames FCS Errored Frames Jabbers Runts Symbol Errors Undersized Frames	Table on page 383 (“Error Stats (Layer 2 Traffic)”) Table on page 384 (“Error Stats (Layer 3 Traffic)”)
Remote Fault Detect Remote Fault Seconds	Table 69 on page 386 (“AutoNeg Status results”) Table 70 on page 387 (“1 Gigabit Ethernet Optical AutoNeg Status results”)
Rx IGMP Frames	Count of the number of IGMP frames received since the last test start or restart.
Block Error Rate (PCS)	The ratio of errored blocks to total blocks since the last restart of the test. *Only applicable when running 40 GigE and 100GigE applications.*
Block Error Secs (PCS)	Count of the number of seconds during which errored blocks were received. *Only applicable when running 40 GigE and 100GigE applications.*
Rx Q-in-Q Frames Rx VLAN Frames Total Received Frames Transmitted Frames	Table 44 on page 359 (“L2 Link Counts results”)

Table 84 Physical/Link Stats results (Continued)

Test Result	For Descriptions, Refer to....
SVLAN ID Total Rx Frame Bytes Total Rx Mbps, Cur L1 Total Util, % Avg Total Util %, Cur Total Util %, Min Total Util %, Peak VLAN ID	Table 43 on page 355 ("L2 Link Stats results")

All Streams Transport results

Table 85 lists the results provided in the All Streams Transport result group, All category. In addition to the test results provided for each discovered stream, you can observe details for a particular stream, such as the source IP address, source port, and encapsulation settings by selecting the stream, and then pressing the **Stream Details** button.

Table 85 All Streams Transport results

Test Result	Explorer	Analyzer	Description
# Streams Analyzed	√	√	Displays the number of discovered streams that are currently being analyzed using either the Explorer or the Analyzer application.
#Prgs	√	√	For MPTS streams, displays the number of programs carried in each discovered stream.
Destination IP Address	√	√	Displays the destination IP address carried in each discovered stream.
Dist. Err Cur		√	Displays a total count of instances where the distance errors fell below the Distance Error threshold during the last test interval. This result is only available when analyzing *RTP encapsulated* video streams.
Dist. Err Max		√	Displays the maximum number of distance errors measured in a test interval since starting or restarting the test. This result is only available when analyzing *RTP encapsulated* video streams.
Dist. Err Tot		√	Displays a total count of instances where the distance errors fell below the Distance Error threshold since starting or restarting the test. This result is only available when analyzing *RTP encapsulated* video streams.
IP Chksum Errors	√	√	Displays a count of instances when the expected IP checksum is not equal to the checksum carried in a received packet for all analyzed streams since starting the test.
L1 Mbps	√	√	Displays the Layer 1 bandwidth utilized by each discovered stream (in Mbps).
Max Loss Period		√	Displays the value for the longest loss period detected since starting or restarting the test. This result is only available when analyzing *RTP encapsulated* video streams.

Table 85 All Streams Transport results (Continued)

Test Result	Explorer	Analyzer	Description
MDI DF Cur		√	Displays the current media delivery index delay factor (MDI-DF). The current count is an average of the measurements taken during each test interval since starting or restarting the test. This result is only applicable if your instrument includes the MDI option and if analyzing *CBR* video streams (not available for VBR or MSTV streams).
MDI DF Max		√	Displays the maximum media delivery index delay factor (MDI-DF) detected since starting or restarting the test. This result is only applicable if your instrument includes the MDI option and if analyzing *CBR* video streams (not availabe for VBR or MSTV streams).
MDI MLR Cur		√	Displays the current media delivery index loss rate (MDI MLR). For RTP encapsulated video streams, the current MLR is calculated by counting the number of lost IP packets during the last test interval, and multiplying this number by seven. If a stream is not RTP encapsulated, this result is the same as the CC Lost Count. This result is only applicable if your instrument includes the MDI option and if analyzing *CBR* video streams (not availabe for VBR or MSTV streams).
MDI MLR Max		√	Displays the current media delivery index loss rate (MDI MLR) declared since starting or restarting the test. This result is only applicable if your instrument includes the MDI option and if analyzing *CBR* video streams (not availabe for VBR or MSTV streams).
Min Loss Distance		√	Displays the value for the shortest loss period detected since starting or restarting the test. This result is only available when analyzing *RTP encapsulated* video streams.
Name	√	√	Displays the name of each discovered stream.
OoS Pkts Cur		√	Displays a count of out of sequence frames detected during the current test interval. This result is only available when analyzing *RTP encapsulated* video streams.
OoS Pkts Max		√	Displays the maximum value for the `OoS Pkts Cur` result since starting or restarting the test.This result is only available when analyzing *RTP encapsulated* video streams.
OoS Pkts Tot		√	Displays a count of out of sequence frames detected since starting or restarting the test. This result is only available when analyzing *RTP encapsulated* video streams.
Period Err Cur		√	Displays the number of loss period errors detected during the last test interval. A loss period error is declared whenever the loss period exceeds the Loss Period threshold. This result is only available when analyzing *RTP encapsulated* video streams.
Period Err Max		√	Displays the maximum value for the `Period Err Cur` result since starting or restarting the test. This result is only available when analyzing *RTP encapsulated* video streams.
Period Err Tot.		√	Displays the total number of loss period errors detected since starting or restarting the test. This result is only available when analyzing *RTP encapsulated* video streams.

Table 85 All Streams Transport results (Continued)

Test Result	Explorer	Analyzer	Description
Pkt Jitter Cur (ms)	√	√	Displays the current packet jitter measured for received packets during the last test interval, calculated in milliseconds. When running Analyzer applications, if the stream is RTP encapsulated, this is derived using the RTP header. This result is only applicable to CBR streams (not availabe for VBR or MSTV streams).
Pkt Jitter Max (ms)	√	√	Displays the maximum packet jitter measured for received packets since the last test restart, calculated in milliseconds. When running Analyzer applications, if the stream is RTP encapsulated, this is derived using the RTP header. This result is only applicable to CBR streams (not availabe for VBR or MSTV streams).
Pkt Loss Cur	√	√	Displays the current number packets lost within the last test interval.
Pkt Loss Max	√	√	Displays the maximum packet lost measured during a single test interval since starting or restarting the test.
Pkt Loss Peak	√	√	Displays the maximum value recorded for the `Pkt Loss Cur` result since starting the test.
Pkt Loss Tot	√	√	Displays the total number of packets lost since starting the test.
Port	√	√	Displays the destination UDP port number carried in each discovered stream.
RTP Present	√	√	For each discovered stream, Yes indicates that an RTP header is present; No indicates that no RTP header is present.
RUDP Packet Count		√	Displays the number of received RUDP unicast retry media packets. It appears only when using MSTV protocol in SPTS Analyzer.
Stream Type		√	Displays the type of stream (CBR or VBR) for each discovered stream.
Sync Losses Tot.		√	Displays a count of the number of instance when synchronization was lost with the MPEG since starting or restarting the test.
Sync Byte Err Tot.		√	Displays the total number of sync byte errors detected since starting or restarting the test.
Sync Byte Err Cur		√	Displays the current number of sync byte errors detected during the last test interval.
Sync Byte Err Max		√	Displays the maximum number of sync byte errors detected during a single test interval since starting or restarting the test.
Total L1 Mbps	√	√	Displays the cumulative Layer 1 bandwidth utilized by all discovered streams (in Mbps).
UDP Chksum Errors	√	√	Displays a count of instances when the expected UDP checksum is not equal to the checksum carried in a received packet for all analyzed streams since starting the test.

All Streams Video/All Program Video results

Table 86 lists the results provided in the All Streams Video result group (All category), and in the Stream result group (All Programs Video result category). The All Programs Video result category only appears when running MPTS (Multiple Program Transport Stream) applications.

Table 86 All Streams Video and All Programs Video results

Test Result	MPTS Explorer	MPTS Analyzer	SPTS Explorer	SPTS Analyzer	Description
Name	√	√	√	√	For descriptions, see Table 85 on page 400 ("All Streams Transport results")
Destination IP Address	√	√	√	√	
Port	√	√	√	√	
L1 Mbps	√	√	√	√	
#Prgs	√	√			
IP Chksum Errors	√	√	√	√	
UDP Chksum Errors	√	√	√	√	
Total L1 Mbps	√	√	√	√	
# Streams Analyzed	√	√	√	√	
Transport ID				√	Displays the transport stream ID carried in the PAT for each discovered stream. (not availabe for MSTV streams)
Prog No.				√	Displays the program number carried in the PAT for the stream. (not availabe for MSTV streams)
PMT PID				√	Displays the program ID for the PMT (Program Map Table) (not availabe for MSTV streams)
#PIDs				√	Displays the total number of PIDs for a particular program.
Prog Mbps Cur				√	Displays the current bandwidth utilized by the program expressed in megabits per second. This measurement is an average taken during the current test interval.
Prog Mbps Min				√	Displays the minimum bandwidth utilized by the program expressed in megabits per second since starting or restarting the test.
Prog Mbps Max				√	Displays the maximum bandwidth utilized by the program expressed in megabits per second since starting or restarting the test.
Sync Losses Tot.		√			Displays a count of the number of instances when synchronization was lost with the MPEG since starting or restarting the test.

Table 86 All Streams Video and All Programs Video results (Continued)

Test Result	MPTS Explorer	MPTS Analyzer	SPTS Explorer	SPTS Analyzer	Description
Sync Byte Err Tot.		√			Displays the total number of sync byte errors since starting or restarting the test.
Sync Byte Err Cur		√			Displays the current number of sync byte errors detected during the last test interval.
Sync Byte Err Max		√			Displays the maximum number of sync byte errors detected during a single test interval since starting or restarting the test.
PCR Jitter Max				√	Displays the maximum PCR jitter during a single test interval since starting or restarting the test. (not availabe for MSTV streams)
PCR Jitter Cur				√	Displays the current PCR jitter measured as an average taken during the last test interval, in milliseconds. (not availabe for MSTV streams)
CC Err Tot.				√	Displays the total number of continuity counter errors since starting or restarting the test.
CC Err Cur				√	Displays the number of continuity counter errors detected during the last test interval.
CC Err Max				√	Displays the maximum number of continuity counter errors detected during a single test interval since starting or restarting the test.
Transp. Err Tot.		√		√	Displays the maximum number of transport errors detected during a single test interval since starting or restarting the test.
Transp. Err Cur		√		√	Displays the number of transport errors detected during the last test interval.
Transp. Err Max		√		√	Displays the maximum number of transport errors detected during a single test interval since starting or restarting the test.
PAT Err Tot.		√		√	Displays the maximum number of PAT errors detected during a single test interval since starting or restarting the test. (not availabe for MSTV streams)
PAT Err Cur		√		√	Displays the current number of PAT errors detected during the last test interval. (not availabe for MSTV streams)

Table 86 All Streams Video and All Programs Video results (Continued)

Test Result	MPTS Explorer	MPTS Analyzer	SPTS Explorer	SPTS Analyzer	Description
PAT Err Max		√		√	Displays the maximum number of PAT errors detected during a single test interval since starting or restarting the test. (not availabe for MSTV streams)
PMT Err Tot.				√	Displays the maximum number of PMT errors detected during a single test interval since starting or restarting the test. (not availabe for MSTV streams)
PMT Err Cur				√	Displays the current number of PMT errors detected during the last test interval. (not availabe for MSTV streams)
PMT Err Max				√	Displays the maximum number of PMT errors detected during a single test interval since starting or restarting the test. (not availabe for MSTV streams)
PID Err Tot.				√	Displays the total number of PID errors detected since starting or restarting the test.
PID Err Cur				√	Displays the current number of PID errors detected during the last test interval.
PID Err Max				√	Displays the maximum number of PID errors detected during a single test interval since starting or restarting the test.

All Streams Complete results

You can observe results associated with transport and video streams by selecting the All Streams Complete result group, All category. Each of the results displayed in this view is documented in Table 85 on page 400 (“All Streams Transport results”) and Table 86 on page 403 (“All Streams Video/All Program Video results”).

Individual stream results

In addition to the All Streams result views, you can observe results for a particular stream by setting the result group to the stream number. The streams are numbered in the order that they appear in the All Streams view.

Each of the results displayed in this view is documented in Table 85 on page 400 ("All Streams Transport results") and Table 86 on page 403 ("All Streams Video/All Program Video results"); however, the result names may be slightly different because in many instances they did not need to be abbreviated. For example, the `Packet Loss, Peak` result that appears for a particular stream provides the same data that is provided by the `Pkt Loss Peak` result in the All Streams view.

Stream and Program PID results

When running MPTS Analyzer applications, you can observe test results associated with the PIDs *for each analyzed program*. When running SPTS Analyzer applications, you can observe results associated with the PIDs in *each analyzed stream*. The PID, PID Type (Audio, Video, PMT, or PAT), bandwidth utilized, and error counts are provided for each PID. Table 87 lists each of the PID results.

Table 87 PID results

Test Result	Description
PID	Displays the PID number.
Type	Displays the PID type (`Audio, Video, PMT, or PAT`).
Mbps	Displays the bandwidth utilized by the PID in Mbps.
CC Err	Displays the number of continuity counter errors detected during the last test interval.
CC Err Max	Displays the maximum number of continuity counter errors detected during a single test interval since starting or restarting the test.
CC Err Tot.	Displays the total number of continuity counter errors since starting or restarting the test.
PID Err	Displays the current number of PMT errors detected during the last test interval.
PID Err Max	Displays the maximum number of PID errors detected during a single test interval since starting or restarting the test.
PID Err Tot.	Displays the total number of PID errors detected since starting or restarting the test.

MSTV results

When running SPTS Analyzer using MSTV protocol, you can observe the MSTV results. There are four groups of results within the MSTV category: Stats, Count, Latency Distribution, and Message Log.

MSTV Stats

Table 88 lists each of the MSTV Stats results.

Table 88 MSTV Stats results

Test Result	Description
ICC Latency with Burst	Average, Current, and Maximum amount of time, in milliseconds, of a MSTV ICC request to the first unicast media packet of the burst video stream.
ICC Latency without Burst	Average, Current, and Maximum amount of time, in milliseconds, of a MSTV ICC request to the first multicast media packet of the video stream.
RUDP Latency	Average, Current, and Maximum amount of time, in milliseconds, of a MSTV RUDP request message to the first unicast retry media packet.
DServer Command Latency	Average, Current, and Maximum amount of time, in milliseconds, of a MSTV command message to its appropriate response, including ICC request and status.
Client Command Latency	Average, Current, and Maximum amount of time, in milliseconds, of a MSTV burst complete message to its AckBurstComplete response.
ICC and RUDP rate	Average, Current, and Maximum bitrate of all ICC media packets, plus uncategorized or late RUDP media packets.

MSTV Count

Table 89 lists each of the MSTV Count results.

Table 89 MSTV Counts results

Test Result	Description
ICC (with Burst) Latency Count	Number of ICC Latency (with burst) measurements done.
ICC (without Burst) Latency Count	Number of ICC Latency (without burst) measurements done.
Total ICC Request Sent	Total number of ICC requests sent.
RUDP Latency Count	Number of RUDP Latency measurements done.

MSTV Latency Distribution

The MSTV Latency Distribution results shows the ICC with burst, ICC without burst, and RUDP latency in graphical form.

MSTV Message Log

The MSTV Message Log provides a listing of significant messages such as join requests, retry requests, leave requests, and errors.

VoIP results

Test results that help you evaluate the quality of the physical, link, transport stream, and voice content layers are available when testing VoIP service. A detailed discussion of the layout and principals behind these results is provided in the "Understanding VoIP test results" on page 232 section of Chapter 10 "VoIP Testing".

Categories discussed in this section include the following:

– "VoIP LEDs" on page 408
– "Content results" on page 409
– "Transport results" on page 410
– "Transaction Log results" on page 411
– "Miscellaneous measurements" on page 411
– "Ethernet results" on page 413
– "Graph results" on page 413

VoIP LEDs

Table 90 describes the LEDs provided during VoIP testing. Only the LEDs that are applicable for your test appear in the LED panel.

If the instrument loses any of the LED events, the green Status LED extinguishes, and the red Alarm LED in the history column illuminates indicating an error condition has occurred. For details, refer to "Understanding the LED panel" on page 232 of Chapter 10 "VoIP Testing".

Table 37 describes the LEDs, and indicates whether each LED is applicable when testing VoIP.

Table 90 VoIP LEDs

LED	Indicates
Call Status	gray – indicates Idle or Unavailable Green – indicates Conversation in Progress
Frame Detect	Green – Valid frames have been detected. Red – Frames were detected, and then not present for ≥1 second.
IP Packet Detect	Green – An IP Packet has been detected. Red – An IP Packet was detected, and then not present for ≥1 second.

Table 90 VoIP LEDs (Continued)

LED	Indicates
Link Active	Green – Auto-negotiation was successful, and link is established with the instrument's link partner. Red – A link to the instrument's link partner has been lost since the last test restart.
Local Content Rating	This result provides current and history rating indication of the call in progress. Green – indicates MOS Score above configured Pass/Good Content Threshold Red – indicates MOS Score below configured Fail/Poor Content Threshold Yellow – indicates MOS Score between Pass and Fail Content Threshold
Network Up/Down	Green – indicates Network is up (Physical Link is up, IP address obtained (if DHCP enabled), PPPoE UP (if Data Mode is PPPoE) Red – indicates Network is down
Phone Status	Green – indicates Registered (Registered with SIP Proxy/H.323 Gatekeeper/ SCCP Call Manager or No Proxy/Gatekeeper) or Registration In Progress gray – indicates Not Registered
Signal Present	Green – A signal is present. Red – Received signal has been lost since the last test start or restart.
Sync Acquired	Green – Synchronization is established. Red – Synchronization has been lost since the last test restart.

Content results

Content provides current and historic call scores. Table 91 describes the current call score measurements.

Table 91 Current Call Scores

Result	Definition
MOS Conversational Quality	Mean Opinion Score represented as a number and a graphic representation of quality.
MOS Listener Quality	Current, Average, Minimum, and Maximum Listener and conversation quality scores.
R Factor Conversational Quality	Current, Average, Minimum, and Maximum conversation quality R factor

Table 91 Current Call Scores (Continued)

Result	Definition
R Factor Listener Quality	Current, Average, Minimum, and Maximum listener quality R factor
R Factor G.107	Current, Average, Minimum, and Maximum G.107 R factor
R Factor Burst	Current, Average, Minimum, and Maximum burst R factor
R Factor Gap	Current, Average, Minimum, and Maximum gap R factor
Local Content Rating	Current, Average, Minimum, and Maximum conversation quality mean opinion score
Local Content Rating	Overall Local content rating: whether the MOS score is currently within the Threshold.

Table 92 describes the historic call score measurements.

Table 92 Historic Call Scores

Result	Definition
MOS Conversational Quality	Average, Minimum, and Maximum MOS for conversation quality for the entire call.
MOS Listener Quality	Average, Minimum, and Maximum Listener quality actor scores for the entire call.
R Factor Conversational Quality	Average, Minimum, and Maximum conversation quality R factor for the entire call.
R Factor Listener Quality	Average, Minimum, and Maximum listener quality R factor for the entire call.
R Factor G.107	Average, Minimum, and Maximum G.107 R factor for the entire call.
R Factor Burst	Average, Minimum, and Maximum burst R f actor for the entire call.
R Factor Gap	Average, Minimum, and Maximum gap R factor for the entire call.
Local Content Rating	Overall Local content rating: whether the MOS score was within the threshold at any point during the call.

Transport results

This category provides quality of service and Stats/Counts.

QoS results

These results report local and remote quality of service results. Table 93 describes the QoS results.

Table 93 Transport QoS results

Result	Definition
Audio Delay	The end to end delay in milliseconds. Current: measured in the last second. Minimum/Maximum: since the beginning of the call QoS: whether the delay has crossed the threshold in the last second. History: the delay has crossed the threshold during any given second so far.

Table 93 Transport QoS results (Continued)

Result	Definition
Jitter	The deviation in packet arrival times, in milliseconds. Current: measured in the last second. Minimum/Maximum: since the beginning of the call QoS: whether the jitter has crossed the threshold in the last second. History: the jitter has crossed the threshold during any given second so far.
Lost packets	Count: number of packets lost Percent: Percentage of packets lost so far from the beginning of the call. QoS: whether the percent has crossed the threshold in the last second. History: whether the percentage crossed the threshold during any given second so far.

NOTE:

The Delay results, Remote Jitter results, and Remote Lost Packets are only provided if the RTCP signaling is active.

Stats/Counts results

These results provide audio throughput stats.Table 94 describes the throughput results.

Table 94 Transport Stats/Counts results

Result	Definition
Local Rate Tx	The local transmit rate
Local Rate Rx	The local receive rate
Bytes Tx	Total number of bytes transmitted
Bytes Rx	Total number of bytes received
Packets Tx	Total number of RTP packets transmitted
Packets Rx	Total number of RTP packets received
Out of Sequence	Total number of packets that arrive out of sequence
Lost Audio Packets	The total number of lost audio packets
Remote Bytes Tx	Total number of bytes transmitted from the remote end
Remote Packets Tx	Total number of RTP packets transmitted from the remote end

Transaction Log results

A running list of all signalling and call status transactions with the far-end.

Miscellaneous measurements

This category provides measurements and call stats.

Measurement results

Table 95 describes the miscellaneous results for the audio path.

Table 95 Miscellaneous results

Result	Definition
Audio Jitter Buffer Replayed	Any time the jitter buffer is queried for a packet to play out and it returns null, this counter is incremented.
Audio Jitter Buffer Dropped	If two packets with different timestamps end up with the same calculated play out (due to a shift in the jitter buffer window), the packet will be discarded and this counter will be incremented.
Delay, Network	Time, in milliseconds, needed to travel the network
Delay, Encoding	Time, in milliseconds, needed to convert samples in selected codec form
Delay, Packetization	Number of milliseconds needed to fill the frame(s) comprising one RTP data packet
Delay, Buffering	Time, in milliseconds, that the data was held in a jitter buffer
Delay Total	Total of all delays
% of Total Delay, Network	The percent of the total delay that is related to network delay
% of Total Delay, Encoding	The percent of the total delay that is related to encoding delay
% of Total Delay, Packetization	The percent of the total delay that is related to packetization delay
% of Total Delay, Buffering	The percent of the total delay that is related to buffering delay
Mic Power Level	The microphone power level, in dBm, coming into the codec. **NOTE**: The microphone power level applies to the level coming into the codec. It is not tied to actual availability of a microphone.
Speaker Power Level	The speaker power level, in dBm, coming out of the codec. **NOTE**: The speaker power level applies to the level coming out of the codec. It is not tied to actual availability of a speaker.

Call Stats results

This category provides results for the current call. Table 96 describes the call info results.

Table 96 Call Stats results

Result	Definition
Call Duration	Length of time for the current call.
Remote IP	The IP address of the incoming call
Remote alias	The alias of the incoming call
Audio Codec Rx	The Audio decoder type used for decoding.
Speech per Frame Rx	The speech per frame received
Audio Codec Tx	The Audio codec being use for transmit
Speech per Frame Tx	The speech per frame being transmitted
RTCP Used	Indicates whether RTCP was used for the Audio path

Table 96 Call Stats results (Continued)

Result	Definition
Silence Suppression	Indicates whether silence suppression is enabled on the far-end.

Ethernet results

This category provides Ethernet Stats, Capture info, and Auto Negotiation status.

Stats results

The Ethernet Stats category provides stats for the physical interface, such as whether signal is present, any code violations, number of transmitted and received frames, and so on.

Capture results

The Capture category provides a count of the number of packets processed, and displays a gauge indicating the percent of the buffer that is filled with captured packets.

Auto Neg Status

This category provides Auto Negotiation Status. It includes stats such as whether the link is pause, FDX, or HDX capable and whether a remote fault was received.

Graph results

The graphical results provide Audio Throughput, Local Audio Delay, Current Audio Jitter, and Current Lost Audio Packets.

Graphical results

The Graphs result group provides test results such as Latency (RTD), Throughput, Instantaneous Packet Jitter, and Errors graphically. When viewing results graphically, a legend is provided under the graph with colors indicating what each color represents on the graph. For graphs that display time, absolute time is used.

You can customize the graphs to suit your needs by doing the following:

– To simplify the graph, you can select the legend, and then choose the data that you want to observe, and hide the rest.
– If you are running a multiple streams application, you can select the legend, and then choose the data that you want to observe for each analyzed stream and hide the rest.

Graphs require significant system resources; therefore, you can optionally disable automatic graph generation if you intend to run other resource intense applications.

To disable graph generation

Step1 On the Main screen, select **Tools > Customize ....**

The Customize User Interface Look and Feel screen appears.

Step2 Clear the **Generate Graphs** setting, and then select **Close** to return to the Main screen.

The MSAM will not automatically generate graphs. You can select the Generate Graphs setting at any time to resume automatic graph generation.

Histogram results

The Histogram result category provides a display of test results in a bar graph format. Histograms enable you to quickly identify spikes and patterns of errors over a specific interval of time (seconds, minutes, or hours).

A sample histogram is provided in Figure 122.

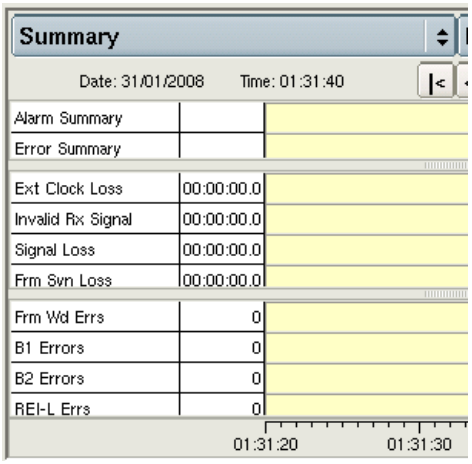


Figure 122 Sample histogram

Results are updated once per second.

NOTE:

Histograms are best viewed using full-sized result window. See “Changing the result layout” on page 4.

Event Log results

The event log result category provides a display listing any significant events, errors or alarms that occur during the course of your test. The log displays the value for each error or alarm, and provides the date and time that the error or alarm occurred.

Events are updated once per second. For instructions on customizing your event log display, see “About the Event log” on page 5.

NOTE:

Event logs are best viewed using full-sized result window. See “Changing the result layout” on page 4.

Time test results

The Time category provides the current date, time, and the time elapsed since the last test start or restart. Table 97 describes each of the Time results.

Table 97 Time results

Result	Description
Current Date	Current day and month.
Current Time	Current time of day in hours, minutes, and seconds (hh:mm:ss).
Test Elapsed Time	Amount of time in hours, minutes, and seconds (hh:mm:ss) since the last test restart.

14

Troubleshooting

If you experience problems when testing using your instrument, you may be able to solve these problems on your own after referring to this section. If you experience significant problems with the module, call the Technical Assistance Center (see “Technical assistance” on page xxiv).

This chapter describes how to identify and correct issues encountered when testing using the instrument. Topics discussed in this chapter include the following:

– “Before testing” on page 418
– “Performing tests” on page 418
– “Upgrades and options” on page 422

Before testing

The following section addresses questions that may be asked about assembling the various components before testing.

The test application I need is not available

When testing using an MSAM, only the applications for *currently inserted PIMs* will appear on the Test menu. For example, if an SFP and XFP PIM are inserted in the MSAM chassis, you will not see DS1 applications. Other applications, such as the Mac-in-Mac applications only appear if you purchased the associated testing option.

Resolution

Insert the appropriate PIM for the application.

Can I hot-swap PIMs?

No, PIMs are not hot-swappable.

Resolution

You must turn the BERT module OFF before inserting or swapping PIMs.

How can I determine whether I need to swap a PIM or swap SFP transceivers?

Tables listing the line rates supported by each PIM are provided in the *Getting Started Manual* that shipped with your instrument or upgrade. Details concerning each of the JDSU recommended optics (transceivers) are available on the instrument itself (by selecting the corresponding option from the Help menu). You can also observe details for the currently inserted SFP or XFP on the Interface setup tab of the Dual Module Carrier, Transport Module, and MSAM user interface.

I am receiving unexpected errors when running optical applications

SFP transceivers are designed for specific interfaces and line rates.

Resolution

Verify that the SFP you inserted into the PIM is designed to support the interface you are connected to for testing. This information is provided on the Interface setup tab of the Dual Module Carrier, Transport Module, and MSAM user interface.

Performing tests

The following section addresses questions that may be asked about performing tests using the Dual Module Carrier, Transport Module, and MSAM.

Optical Overload Protection message

When in optical mode, the instrument displays a warning that the Optical Overload Protection is activated, or the instrument does not detect a signal.

Resolution

Applied power must not exceed the power level specified in the vendor specifications provided for your SFP or XFP.

User interface is not launching

The BERT icon is highlighted in yellow, but the user interface is not launching.

Resolution

Press the Results or the Start/Stop key to display the user interface.

Inconsistent test results

I am getting inconsistent test results.

Resolution

Verify the following:

– Verify that your test leads are good and are connected properly for the test you are performing.
– Verify that the correct timing source is selected on the Interface setup screen.
– Verify that the correct line interface is selected.
– Verify that the correct mapping, tributaries, and analysis rates are selected.

Result values are blank

Why are the result values blank?

Resolution

Results are blank if gating criteria have not been met. Criteria examples include Signal Present, Frame Sync Present, Pointer Present, and BERT Pattern Sync Present.

Unit on far end will not loop up

The unit on the far end will not respond to a Loop Up command.

Resolution

Verify that the application running on the far end is not configured to automatically transmit traffic when the laser is turned on. If so, it can not respond to a Loop Up command. Turn the setting off.

A receiving instrument is showing many bit errors

I am transmitting an ATP payload carrying a BERT pattern, and the receiving instrument is showing a large number of bit errors.

Resolution

Verify that the receiving instrument is not using a Version 1 Transport Module. You can determine this by checking the serial number for the module. If there is no V2 or V3 prefix for the serial number, you are using a version 1 module.

Even when running software version 8.x, version 1 Transport Modules will not support ATP payloads carrying BERT patterns. Version 2 and Version 3 Transport Modules do support the payloads.

RFC 2544 or FC Script button does not appear

The the **RFC 2544** or **FC Script** button does not appear on the Main screen.

Resolution

Verify the following:

– Payload analysis is ON for your current test application. You can not run the RFC 2544 or Fibre Channel script when the module is configured to analyze live traffic.
– Traffic is not VPLS or MPLS encapsulated. You can not run the RFC 2544 with VPLS or MPLS encapsulated traffic.
– The module is not configured to run a timed test. You can not run the RFC 2544 or Fibre Channel script during a timed test.

Which MSAM or application module is selected?

When testing using an 8000 and two MSAMs (via a DMC), or an 8000 using multiple application modules, which test is in the foreground, and which is running in the background?

Resolution

On the Main screen, a button appears in the menu bar indicating which DMC slot and port, or which 8000 application module and port is currently selected.

I am transmitting Layer 2 Ethernet traffic with OAM frames at 10 Mbps, but no frames are transmitted or received

When your instrument is configured to transmit Ethernet traffic with OAM frames at a low speed (10 Mbps) and low bandwidth (for example, .001% of the line rate), the instrument gives the OAM frame the priority, and sends it every second. As a result, regular traffic is stalled, because the instrument is only sending the OAM frames at regular intervals. This is expected behavior.

Resolution

Try the following:

– Increase the bandwidth.
– Turn Link OAM and Service OAM OFF.
– Run the test without the OAM frames. Frames will be counted as transmitted and received.

One way delay measurements do not appear

One way delay measurements do not appear on the results pages.

Resolution

Verify the following:

– Are you testing using two GPS time synchronized instruments? Two synchronized instruments are required to ensure accurate measurements. If both units are not synchronized, the instruments will transmit standard ATP test packets (instead of ATP-UTC test packets), and standard round trip delay measurements will be reported instead of one way delay measurements.
– If your instruments are not synchronized, verify that:
  – Both instruments are located within a CDMA network.
  – All connections from the USB port and the BNC connector on the instrument to the CDMA receiver are secure (see “Step 1: Connecting the receivers to your instruments” on page 111).
– If your instruments are synchronized, verify that transmitting instruments are configured to transmit an Acterna payload. If a BERT payload is transmitted, delay can not be measured because the test packets do not carry the required UTC timestamp. Although you must transmit an Acterna payload, you can populate the payload with either a BERT pattern or a fill-byte pattern.

My VoIP call didn’t go through

The VoIP call did not successfully go through.

Resolution

Check your connections to verify that they are hooked up properly.

Check the Ethernet link light on the instrument’s Ethernet jack. It should be green.

Verify the LAN settings (IP address, netmask, DNS name).

Verify the call control. Most equipment uses Fast Connect.

If you *do not* have a gatekeeper, verify the outgoing alias and IP address.

If you *are* using a gatekeeper, verify you are registered with the gatekeeper.

Check with your system administrator to verify that the firewall allows VoIP traffic.

I am emulating a SIP phone but cannot register with the SIP server.

I am emulating a SIP phone but cannot register with the SIP server.

Resolution

In typical networks, the same server handles both registration and placing and receiving calls. However, in some networks, there is a Proxy server that handles SIP messaging for placing and receiving calls, and a registrar that handles registration, which may be in a different domain.

If this is the case, do the following.

– Verify that you specified the “Proxy” on the Proxy Settings menu as the outbound proxy, or the device from which the HST will send and receive all SIP messages (for placing and receiving calls).

– Verify that you specified the “Alias” on the General Settings menu as the SIP server or registrar (the device that keeps track of all the registered devices), using the following format “phone-Number@domain” where domain is either an IP address of the registrar or a literal domain such as “jdsu.com”.

I am running a VoIP test but the delay measurement does not appear.

The delay measurement does not appear.

Resolution

The delay measurement is only displayed if RTCP is supported.

I have very little loss, but a high level of delay on my VoIP test

I have very little loss, but a high level of delay.

Resolution

Check your network. It may be experiencing high traffic.

I have a large amount of jitter in my VoIP test, but no loss or delay.

I have a large amount of jitter, but no loss or delay.

Resolution

Check the setup of your router.

Upgrades and options

The following section addresses questions that may be asked about upgrading or installing test options for the instrument.

How do I upgrade my instrument?

Upgrades are installed from a USB key. Instructions are provided with each software upgrade.

How do I install test options?

Test options are enabled by entering a JDSU provided challenge code. Instructions are provided when you order test options.

Do software and test options move with the Dual Module Carrier, Transport Module, and MSAM or Transport Module?

Test options are available when you connect the Dual Module Carrier, Transport Module, and MSAM or Transport Module to a different base unit; however, the base unit software and BERT (MSAM/Transport Module) software reside on the base unit.

Glossary

Symbols/Numerics

10G — Used to represent 10 Gigabit Ethernet.

10GigE — Used throughout this manual to represent 10 Gigabit Ethernet.

2M — *See E1*. The E1 PIMs are used when testing 2M interfaces.

802.11b — IEEE standard for wireless LANs. You can establish wireless LAN connections to the T-BERD/MTS 8000, 6000A, and 5800 using an 802.11 PCMCIA card.

802.3 — The IEEE specification for Ethernet. 802.3 also specifies a frame type that places the frame length in the Length/Type field of the Ethernet header, as opposed to the DIX Type II frame type which utilizes the Length/Type field to identify the payload Ethertype.

A

AC — Alternating Current. An AC power adapter is supplied with the instrument.

ARP — Address Resolution Protocol. Method for determining a host's hardware address if only the IP address is known. The instrument automatically sends ARP requests during layer 3 IP testing.

ATP — Acterna test packet. A test packet that contains a time stamp and sequence number for measuring round trip delay and counting out-of-sequence frames.

B

BER — Bit Error Rate.

BERT — Bit error rate test. A known pattern of bits is transmitted, and errors received are counted to figure the BER. The Bit Error Rate test is used to measure transmission quality.

C

CCM — Continuity Check Message.

CDP — Cisco Discovery Protocol.

CE — Customer Edge.

CFM — Connectivity Fault Management. Comprises capabilities for detecting, verifying, and isolating connectivity failures in VLANs.

Concat — Concatenated.

CPRI — Common Public Radio Interface

Curr — Current.

D

DA — Destination address.

DAD — IPv6 duplicate address detection. When going through the Multicast Listener Discovery process to obtain or verify a link local address, a device issues a neighbor solicitation using the tentative address to determine if the address is already used. This process is referred to as DAD.

DB-9 — Standard 9-pin RS-232 serial port or connector.

DB-25 — 25-pin RS-232 serial port or connector.

Dec — Decrement.

DHCP — Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses dynamically as needed. Also supports static IP address assignment.

DIX — Digital, Intel, and Xerox. Ethernet Type II frame format.

DSCP — Differentiated Services Code Point. A method for specifying IP packets will be queued while waiting to be forwarded within a router.

E

EDD — Ethernet demarcation device.

EFM — Ethernet First Mile.

Err — Error.

Erred — Errored.

Ethernet — A LAN protocol. Using the instrument, you can test and verify Ethernet network elements and services.

Ethernet link partner — The nearest Ethernet device on a link. The instrument auto-negotiates its capabilities with this device when you initialize a link.

ETS — Ethernet Transport Service. A point-to-point path through a specific component of a switch.

ETSI — European Telecommunications Standards Institute.

F

FCS — Frame check sequence. A value calculated by an originating device and inserted into an Ethernet frame. The receiving device performs the same calculation, and compares its FCS value with the FCS value in the frame. If the values don't match (suggesting the frame is errored), an FCS error is declared. Switching devices will discard the frame.

FDV — Frame Delay Variation. Maximum frame jitter within SLA compliance.

FDX — Full Duplex.

FE — Far End. Used by the ITU performance measures to indicate which end of the network is being tested.

FTD — Frame Transfer Delay. Maximum frame transfer time (source to destination) within SLA compliance.

FTP — File transfer protocol. Protocol used on LANs and the Internet to transfer files.

Frame Loss — Loss of frame synchronization.

G

GARP — Generic Attribute Registration Protocol.

Gate time — Time duration for error measurement. During this period the error source is accumulated if it is an error or recorded if it is an alarm.

GigE — Used throughout this manual to represent Gigabit Ethernet.

Global Addresses — Second IPv6 source address assigned to an interface. The global address is not used locally, and is broader in scope, typically to get past a router. If you use auto-configuration to establish a link, the global address is provided automatically.

GMRP — GARP Multicast Registration Protocol.

GUI — Graphical User Interface. Layout of commands in a user-friendly environment. *See also* UI (user interface).

GVRP — GARP VLAN Registration Protocol.

H

HBER — High bit error ratio.

HDX — Half duplex.

Histogram — Print output of specific results in a bar graph format.

Hz — Hertz (cycles per second).

I

IGMP — Internet Group Management Protocol.

Inc — Increment.

Internet Protocol — Commonly referred to as "IP". Protocol specifying the format and address scheme of packets transmitted over the Internet. Typically used with TCP.

IOS — Internetwork Operating System. Software used on most Cisco Systems routers and current Cisco network switches. The instrument allows you to use the automated TAM test to remotely provision and monitor network elements running this IOS.

IP — *See* Internet Protocol.

IPoE — Internet Protocol over Ethernet. Used on the GUI and through this guide to see the applications used to establish a standard layer 3 (IP) connection.

IPv4 — Internet Protocol Version 4.

IPv6 — Internet Protocol Version 6.

ISM — In-Service Monitoring.

ISO — International Organization for Standardization.

ISP — Internet service provider. A vendor who provides access to the Internet and the World Wide Web.

ITU — International Telecommunications Union based in Geneva, Switzerland.

J

Jabber — An Ethernet frame that exceeds the IEEE 802.3 maximum length of 1518 bytes (or 1522 bytes with a VLAN tag) and contains an errored FCS.

J-Connect — Utility that allows you to detect other JDSU test instruments on a particular subnet, and use a detected instrument's addresses to automatically populate key traffic settings. Also known as JDSU-Discovery.

JDSU Discovery — See J-Connect.

JMEP — JDSU Micro Ethernet Small Form-Factor Pluggable Probe (SFP). A 1310 nm, 1000Base-LX, Gigabit Ethernet SFP transceiver that reduces the need for additional instrumentation.

J-Mentor — Utility provided on the instrument that allows you to capture data for analysis when testing from an Ethernet interface.

J-Proof — Application used to verify Layer 2 Transparency.

J-Scan — Utility used to scan and detect the signal structure and mappings from a SONET or SDH interface. Also referred to in other documents as the Auto-Discovery feature.

Jumbo frame — An Ethernet frame that exceeds the IEEE 802.3 maximum length of 1518 bytes (or 1522 bytes with a VLAN tag). You can transmit jumbo frames using the T-BERD/MTS 8000, 6000A, and 5800.

Just — Justification.

L

LAN — Local Access Network.

LACP — Link Aggregation Control Protocol.

LBM — Loopback Message.

LBR — Loopback Reply.

LCD — Liquid Crystal Display.

LCK — LoCKed defect.

LED — Light emitting diode.

LLB — Line Loopback.

LLC — Logical link control. Three bytes carried in 802.3 frames which specify the memory buffer the data frame is placed in.

LLDP — Link Layer Discovery Protocol.

LiION — Lithium Ion. The instrument can be equipped with a rechargeable Lithium Ion battery.

Link-Local Address — IPv6 address assigned to a device locally in an IP network when there is no other assignment method available, such as a DHCP server. These addresses must always go through duplicate address detection (DAD), even if you manually specify the address. *See also* DAD and Global Addresses.

LOC — Loss of Continuity.

LOF — Loss of Frame. A condition indicating that the receiving equipment has lost frame synchronization.

M

Maintenance Association (MA) — A set of MEPs that are each configured with the same maintenance association identifier (MAID) and MD level, which are established to verify the integrity of a single service instance.

Maintenance Association Identifier (MAID) — An identifier for an MA, unique over the domain, that uses CFM to protect against the accidental concatenate.

Maintenance Domain (MD) — The network or the part of the network for which faults in connectivity can be managed.

MDI — Media Delivery Index (video applications).

MDI-X port — Medium Dependent Interface Crossover port. RJ-45 interface used by Ethernet NICs and routers that requires use of a cross-over cable (MDI-X ports cross transmit and receive lines. An MDI-X port on one device connects to an MDI port on another device. MDI-X interfaces transmit using pins 3 and 6, and receive using pins 1 and 2. The Transport Module supports cable diagnostics of MDI-X interfaces.

Maintenance Entity (ME) — Represents an entity that requires management and facilitates a relationship between two ME group end points.

MEG — Maintenance Entity Group. Includes different MEs that satisfy the following conditions: a) MEs in a MEG exist in the same administrative boundary, b) MEs in a MEG have the same MEG level, or c) MEs in a MEG belong to the same point-to-point or multipoint Ethernet connections.

MEG End Point (MEP) — Marks the end point of an Ethernet MEG that can initiate and terminate OAM frames for fault management and performance monitoring.

MEG Intermediate Point (MIP) — Serves as an intermediate point in a MEG that reacts to certain OAM frames. A MIP does not initiate OAM frames, nor does it take action on the transit Ethernet flows.

Maintenance Association End-Point Identifier (MEPID) — A small integer, unique over a given MA, which identifies a specific MEP.

MFAS — Multi Frame Alignment Signal.

MPEG — Set of standards for compression of audio and video and multimedia delivery developed by the Moving Pictures Expert Group.

MPLS — Multiple Path Label Switching. A mechanism using labels rather than routing tables to transmit layer 3 IP traffic over a Layer 2 Ethernet network.

Msg — Message.

MPD — Mean Path Delay

MPLS — Multiprotocol Label

Switching. A form of frame encapsulation that uses labels rather than routing tables to transmit layer 3 traffic over a

layer 2 Ethernet network.

MPTS — Multiple program transport stream.

MSAM — Multiple Services Application Module. Application module used in combination with the T-BERD / MTS 6000A base unit or a DMC and a
T-BERD / MTS 8000 base unit for testing from a variety of interfaces.

MSC — Mobility Switching Center.

MSPP — MSPP. Multi-service provisioning platform. Typically next generation SONET multiplexors capable of aggregating multiple access technologies such as Ethernet, TDM, and ATM onto a SONET ring.

MSTP — Multiple Spanning Tree Protocol.

Multipat — Multiple patterns. An automated sequence of 5 BERT patterns for three minutes each. The Multipat sequence consists of ALL ONES, 1:7, 2 in 8, 3 in 24, and QRSS.

N

NDF — New data flag.

NE — Near-end. Used by ITU performance measurements to indicate which end of the network is being tested.

NetFlow — NetFlow is a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting IP traffic information.

NID — Network Interface Device. Device located on the customer premises used by carriers to properly demark and manage their network.

NIU — Network Interface Unit. Electronic device at the point of interconnection between the service provider communications facilities and terminal equipment at a subscriber’s premises.

NOC — Network Operations Center.

NSA — Non-service affecting.

O

OAM — Operations, Administration, and Maintenance. The instrument allows you to run link and service layer OAM applications.

OBSAI RP3 — Open Base Station Architecture Initiative Reference Point 3.

ODU — Optical channel data unit.

OOF — Out of framing.

OOM — Out of multi framing.

OOS — Out of sequence.

OPU — Optical channel payload unit.

OTN — Optical Transport Network. Network protocol that facilitates the transmission of different types of client signals, such as SONET, SDH, and Ethernet over a single optical network through the use of an OTN wrapper, which provides the overhead required for proper network management.

OTU1 — Used on the user interface to identify the test applications used for 2.7G OTN testing.

OTU2 — Used on the user interface to identify the test applications used for 10.7G, 11.05G, and 11.1G OTN testing.

OWD — One-Way Delay

P

Packet — Bundle of data, configured for transmission. Consists of data to be transmitted and control information.

Packet Delay Variation — The difference in one-way-delay as experienced by a series of packets.

PAT — Program Association Table.

Pattern sync — The condition occurring when the data received matches the data that is expected for a period of time defined by the pattern selected.

PCAP — File format used for packet captures on the instrument.

PCR — Program Clock Reference.

PDV — Packet Delay Variation. The difference in one-way delay for pairs of packets in a flow.

PE — Provider edge.

PES — Packetized elementary streams. Streams carrying packetized video and audio payloads.

PID — Program ID.

PLM-P — Payload mismatch Path.

PM — Path monitoring.

PMT — Program Map Table.

PPPoE — Point to Point Protocol over Ethernet. PPPoE is used on the GUI and throughout this guide to see the applications used to establish a connection to a PPPoE peer via a login process. The HST can emulate a PPPoE client or server.

Pseudo wires (PW) — Point-to-point connections used to carry each type of service between to PE routers in a VPLS network.

Q

Q-in-Q — Also known as VLAN stacking, enables service providers to use a single VLAN to support customers who have multiple VLANs. Q-in-Q VLANs can also be used to provide virtual access and connections to multiple services available over the ISPs, ASPs, and storage services.

QoS — Quality of Service.

QRSS — Quasi-Random Signal Sequence. A modified 2^20-1 pseudo random test signal, modified for use in AMI circuits.

R

RDI — Remote Defect Indication. A terminal will transmit an RDI when it loses its incoming signal.

REI — Remote Error Indicator.

RFI — Remote Failure Indicator.

RJ 48-11 — Modular telephone jack, typically used for telephones, modems, and fax machines.

RSTP — Rapid Spanning Tree Protocol.

RS-232 — Set of standards specifying electrical, functional and mechanical interfaces used for communicating between computers, terminals and modems.

RTD — Round-Trip Delay. Maximum frame transfer delay when measured at source after signal is looped back from far end.

RTP — Real-time Transport Protocol. Standardized packet format for delivering audio and video over the Internet. MPEG video streams are often encapsulated in RTP packets.

Runt — An Ethernet frame that is shorter than the IEEE 802.3 minimum frame length of 64 bytes and contains an errored FCS, or a Fibre Channel frame that is shorter than the minimum 28 byte frame length containing an errored CRC.

Rx — Receive or receiver or input.

S

SA — 1. Source address. 2. Service affecting.

SD — Signal degradation.

Secs — Seconds.

Service disruption time — The time between Ethernet (maximum inter-frame gap) when service switches to a protect line. The Svc Disruption (us) result in the Link Stats category displays the service disruption time.

SF — Signal fail.

SFD — Start of frame delimiter. Part of an Ethernet frame preamble that indicates that the destination address frame is about to begin.

SFP — Small form-factor pluggable module. Used throughout this manual to represent pluggable optical transceivers (modules).

SLA — Service Level Agreement.

SNAP — SubNetwork Access Protocol. Protocol used in 802.3 frames which specifies a vendor code and an Ethertype. When you transmit pings using the Transport Module, you can transmit 802.3 frames with logical link control (LLC) and SNAP.

SPTS — Single Program Transport Stream.

STP — Spanning Tree Protocol.

SVLAN — Stacked VLAN. Used in Q-in-Q traffic to provide a second encapsulation tag, expanding the number of VLANs available. Often considered the VLAN assigned to the service provider (as opposed to the customer).

Sync — Synchronization.

T

TAM — Test Access Management. Application used to provision network elements using your instrument at a remote location.

TCP — Transmission Control Protocol. Layer 4 protocol that allows two devices to establish a connection and exchange streams of data.

TCP Window Size — The maximum number of bytes that a port can transmit over a TCP connection before being acknowledged by the receiving port.

Term — See Terminate.

Terminate — An application where the instrument is terminating the circuit. In these applications, the instrument sends and receives traffic.

Through — An application where the instrument is used in series with a network circuit to monitor the traffic on that circuit.

TL1 — Language used to manage optical and broadband access infrastructure in North America. TL1 is used in input and output messages that pass between Operations Systems (OSs) and Network Elements (NEs). Using the test access management tool on your instrument, you can establish a connection to an NE, then issue TL1 commands to configure the NE remotely or monitor activity.

TOH — Transport Overhead.

TU — Tributary unit.

Tx — Transmit or transmitter or output.

U

UAS — Unavailable seconds.

UDP — User Datagram Protocol. Layer 4 protocol that offers a limited amount of service when messages are exchanged between devices on an IP network. UDP uses IP to transmit data from one device to another device; however, unlike TCP, UDP does not divide a message into packets, and then reassemble the packets at the far end.

UI — Unit Interval. One bit period at the data rate being measured.

us — Microseconds (also expressed as μs).

USB — Universal Serial Bus. A bus designed to handle a broad range of devices, such as keyboards, mouses, printers, modems, and hubs.

V

VDC — Volts Direct Current.

VLAN — Virtual LAN.

VNC — Virtual Network Computing. A thin client system that enables you to run applications on a VNC server from any other computer connected to the Internet. Using VNC, you can run the instrument from a remote workstation.

VPLS — Virtual Private LAN Service. An MPLS application which provides multi-point to multi-point layer 2 VPN services, allowing geographically dispersed sites to share an ethernet broadcast domain by connecting each site to an MPLS-based network.

W

WAN — Wide area network.

X

XFP — 10 Gigabit Small Form Factor Pluggable Module.

Index

Numerics

10 Gigabit Ethernet WAN testing
  about results 345
  default overhead values 29

1G Pair Status result 353

3.072G optical
  BERT 8, 12
  monitoring 9, 18

802.3ae, overhead values 29

A

Address book, populating 215, 236

Alarm LEDs
  Ethernet 354
  Fibre Channel 354
  IP 354
  IP Video 398, 408
  TCP/UDP 354

Alarm test intervals, IP Video 219

Analyzer applications, IP Video 203

Analyzing MPLS-TP traffic 70–74

Analyzing wander 142

Applications
  IP Video testing 215
  loop back 189
  MiM 27, 28
  Multiple Streams 168
  selecting 2
  TCP/UDP 149
  Triple Play 181

ATP listen port, explained 150

Automated tests
  applications 279
  Fibre Channel 282
  FTP Throughput test 318
  HTTP Throughput test 320
  launching 279
  RFC 2544 282
  saving test report data 336
  specifying external settings 292
  TCP Throughput 321
  TrueSAM 264–278
  VLAN 317

AutoNeg Status results 386

B

BER testing
  3.072G optical 8, 12
  Ethernet results 367
  Ethernet, layer 1 45
  Ethernet, layer 2 68
  Fibre Channel, layer 1 250

BERT results
  Ethernet 367
  Fibre Channel 367

Buffer capacity, captured packets 94

Bursty loads, transmitting 65

Byte pattern filter 62

C

Cable diagnostics
  about 32
  running 32
  test results explained 351
  viewing measurements 33

Call control standard 238

Calls
  placing 243
  receiving 243–244

Capturing packets
  about 93, 244
  based on a trigger 97–99
  buffer capacity 94
  Capture toolbar 95, 244
  capturing packets 96, 245
  estimated time to save buffer data 101
  exporting buffer data 100

packet slicing 94
saving buffer data 100
specifying filter settings 95, 244
test results 385, 386
test traffic and control plane traffic, defined 93
VoIP 241

CDMA receiver 107, 111
results 368

CJPAT pattern 69, 258

Collapsing measurements 4

Compliance information xxiv

Configuring tests 2

Connecting
instrument to circuit 3

Constant loads, transmitting 64

Conventions xxiii

CRPAT pattern 69, 258

CSPAT pattern 69, 258

Custom test results
creating 5
maintaining 5

Customer services, technical assistance xxiv

D

Delay, measuring
Fibre Channel 259
MiM 131

Diagnostics, running cable 32

Discovering
other JDSU instruments 36
traffic using J-Profiler 136

Discovering network devices 40, 42

Displaying test results 4

E

Encapsulation
MiM 127, 129
MPLS 30, 79, 80
Q-in-Q 50, 55, 79, 237
VLAN 50, 54, 79, 237
VPLS 29, 50, 55

Error Stats results
Ethernet, layer 1 381
Ethernet, layer 2 383
Ethernet, layer 3 384

Errors, inserting Fibre Channel 259

Ethernet test results
AutoNeg Status 386
Error Stats, layer 1 381
Error Stats, layer 2 383
Error Stats, layer 3 384
L2 BERT Stats 367
L2 Filtered Counts 365
L2 Filtered Stats 361
L2 Link Counts 359
L2 Link Stats 355
LEDs 347
OAM 369, 371, 372, 373
Ping 378
Signal 354, 399
Transparency 366

Ethernet testing
about 147
automated 282
BER testing, layer 1 44, 45
BER testing, layer 2 68
capturing packets 93, 244
classic RFC 2544 test 291
features and capabilities 22
filter settings 56
frame settings 49, 237
interface settings 46, 79
Layer 2 transparency 74
monitoring traffic 70, 133
MPLS 30
OAM service layer 119
test results 341–345, 345–386
traffic loads 64
transmitting traffic 68
verifying layer 2 transparency 74
VPLS 29

Event logs, about 5

Expanding measurements 4

Explicit Fabric/N-port logins 249

Explorer applications, IP Video 203

Exporting wander data 145

F

Fault results 352

Features and capabilities
Ethernet 22
Fibre Channel 248
IP Video testing 205
Jitter and Wander 140
Multiple Streams testing 166
PDH 140
T-Carrier 140
TCP/UDP testing 148
Triple Play testing 166

Fibre Channel test results
Login Status 388

Fibre Channel testing
about N_Port login 249
applications 250
automated 282
features and capabilities 248
filter settings 255
frame settings 254
implicit and explicit logins 253
inserting errors 259
interface settings 252
layer 1 BER 250
measuring delay 259
measuring service disruption 258
monitoring traffic 260
running automated 282
topologies 253
traffic loads 256
transmitting patterns 257
transmitting traffic 256

Filter settings
Ethernet 56
Fibre Channel 255
for packet capture 95, 244
IP 85, 87
IP Video 217, 237
MiM traffic 129
TCP/UDP 155
VoIP 241

Frame settings
Ethernet 49, 237
Fibre Channel 254
MiM traffic 126

FTP Throughput test, automated 318

G

G.826 results 384

Graphs, about 5

H

H.323 238, 239, 240

Help, technical assistance xxiv

Histograms
about 4
viewing 5

HTTP Throughput test, automated 320

I

IGMP settings, IP Video 221

Incrementing
MAC addresses 178
VLAN IDs 178

Interface settings
Ethernet 46, 79
Fibre Channel 252
IP Video 217, 237

IP Config Status results 377

IP test results
IP Config Status 377
L3 Config Status 377
L3 Filter Counts 377
L3 Filter Stats 376
L3 Link Counts 375
L3 Link Stats 374

IP testing
automated 282
capturing packets 93, 244
classic RFC 2544 test 291
filter settings 85, 87
monitoring traffic 92
packet settings 83, 86
Ping 89
running Traceroute 91
traffic loads 64
transmitting 88

IP Video test results
customizing the display 214
LEDs 398, 408
MSTV 407
navigating the display 214
observing physical and link statistics 223
observing stream statistics 224
static and dynamic, explained 213
understanding 207

IP Video testing
about Analyzer applications 203
about Explorer applications 203
about MPTS 203
about PES 226
about RTP encapsulation 227
about signaling tables 226
about SPTS 203
about UDP encapsulation 227
action buttons 206, 231
alarm test intervals 219
Analyzer applications, features 212
applications 215
button colors, explained 208
button colors, illustrated 208
Explorer applications, features 212
features and capabilities 205
filter settings 217, 237
graphical user interface, about 205, 231
IGMP settings 221
interface settings 217, 237
joining streams 222
layered results view 207, 233
leaving streams 187, 224
LEDs 206, 232
network architecture, explained 225
network architecture, illustrated 202
observing physical and link statistics 223
observing stream statistics 224
populating address book 215, 236
quality buttons, explained 207
restart button 206
result threshold settings 219
stream icons, explained 211
streams results view 210
symptoms, source content issues 225
symptoms, transport network problems 226
typical encapsulation, illustrated 203, 231
understanding MPEG streams 202, 230
understanding test results 207

IPTV encapsulation, illustrated 203, 231

J

J-Connect
about 36
discovering instruments 37
discovering JDSU instruments 36
observing instrument details 39
prerequisites 36

JDSU Discovery 36
discoverable instruments 36
discovering instruments 37
observing details for an instrument 39
prerequisites 36
refresh soft key 38
sorting instruments 38

Jitter testing
about 140
features and capabilities 140

Jitter testing, packet 106

Joining video streams 222

J-Profiler
about 136
test results 395

J-Proof testing
See Transparency testing 74

J-QuickCheck, running before RFC 2544 298

L

L2 BERT Stats results 367

L2 Filtered Counts results 365

L2 Filtered Stats results 361

L2 Link Counts results 359

L2 Link Stats results 355
L3 Config Status results 377
L3 Filter Counts results 377
L3 Filter Stats results 376
L3 Link Counts results 375
L3 Link Stats results 374
L4 Filter Counts results 395
L4 Filter Stats results 395
L4 Link Counts results 395
L4 Link Stats results 393
Labels
  specifying MPLS 49, 237
  specifying VPLS 49, 237
Laser, turning ON or OFF 3
Layer 1 BER testing
  See Ethernet testing or Fibre Channel testing
Layer 2 testing
  See Ethernet testing or Fibre Channel testing
Layer 2 transparency
  about loop backs 75
  configuring near end 75
  initiating the loop back 77
  observing results 78
  starting the frame sequence 78
  using Quick Config 76
  verifying 74
Layer 3 testing
  See IP testing
Layer 4 testing
  See TCP/UDP testing
Layout, changing result 4
LBM messages, sending 125
Leaving video streams 187, 224
LEDs
  alarm 354, 398, 408
  Ethernet 347
  IP Video 398, 408
  MiM 126
  Multiple Streams 159, 169
  Triple Play 182
Link connectivity test 45
Loads
  about Ethernet traffic 64
  transmitting bursty 65
  transmitting constant 64
  transmitting ramped 67
Login Status results 388
Logs
  about event 5
Loop back testing
  about transparent L2 75
  action buttons 194
  address swapping 191
  applications 189, 194
  ARP settings 191
  filter criteria 191
  key concepts 191
  messages 194
  MPLS traffic 192
  specifying unit ID 195
  TCP/UDP traffic 193
  terminology 190
  using LLB 195
  using Loop Up 197
  VLAN and Q-in-Q traffic 192
  VPLS traffic 192

M

MAC addresses, incrementing for multiple streams 178
MAC-in-MAC testing, *See* MiM testing
MDI/MDIX Pair Status result 351
Measurements
  cable diagnostic 33
  expanding and collapsing 4
Measuring
  IP packet jitter 106
  packet jitter 106
  round trip delay *See* Delay
  service disruption time, *See* Service disruption time
Messages, PPPoE 82
MGCP, defined 239
MiM testing
  about results 345
  applications 27, 28
  configuring tests 126
  filter settings 129
  frame settings 126
  inserting errors 131
  inserting pause frames 131
  LEDs 126
  measuring delay 131
  OAM settings 130
  test results 125
  traffic loads 130
  transmitting traffic 130
Monitoring
  3.072G optical 9, 18
  Fibre Channel traffic 260
  layer 2 traffic, Ethernet 70, 133
  layer 2 traffic, Fibre Channel 260
  layer 3 traffic, IP 92
MPEG video transport streams
  understanding 202, 230
MPLS testing
  about results 346
  encapsulation settings 79, 80
  loop back settings 192
  overview 30
  specifying labels 49, 237
MPLS-TP testing
  results 359, 361
  running 70–74
MPTS, about 203
MSTV results 407
Multiple Streams testing
  about test results 159, 170
  applications 168
  capturing packets 93, 244
  enabling streams 172
  features and capabilities 166
  graphical results, changing properties 171
  graphical results, viewing 159, 170
  incrementing MAC addresses 178
  incrementing VLAN IDs 178
  LEDs 159, 169
  looping back streams 187
  Pipe display 169
  running TCP Host script 187
  specifying common traffic characteristics 175

specifying layer 2 settings 177
specifying layer 3 settings 179
specifying layer 4 settings 179
specifying load types 173
specifying load unit 175
transmitting streams 180

Multiple tests, running 5

N

Network discovery 40, 42

NewGen
configuring layer 2 tests 126
inserting errors 131
inserting pause frames 131
measuring packet jitter 131
measuring round trip delay 131
measuring service disruption time 132
monitoring traffic 132
test results, about 125
transmitting layer 2 traffic 130

NewGen testing, about results 346

O

OAM testing
about service layer 119
results 369, 371, 372, 373
sending LBM messages 125
specifying settings 120
turning RDI analysis ON 125

One way delay
measuring 107–118
results 360, 363

Optimizing RFC test time 290

OTN testing
inserting defects 16, 106

P

Packet jitter, measuring IP 106

Packet settings, IP 83, 86

Packet slicing, about 94

Pair Skew result 353

Parameters, specifying test 2

Patterns
CJPAT 69, 258
CRPAT 69, 258
CSPAT 69, 258
transmitting layer 2 Ethernet 69
transmitting layer 2 Fibre Channel 257

PBB testing
See MiM testing

PDH testing
features and capabilities 140

Performance
G.826 results 384

PES, explained 226

Ping
results 378
testing 89, 378

Placing calls 243

Populating custom results 5

Ports
ATP listen 150
well known TCP/UDP 153

PPPoE testing
messages 82
See also IP testing

PTP
analyzing traffic 133–136
results, link counts 390
results, link stats 391

Q

Q-in-Q testing
encapsulation settings 50, 55, 79, 237
specifying SVLAN and CVLAN 49, 237

Quick Config settings 28

R

Ramped loads, transmitting 67

RDI analysis, turning ON 125

Receiving calls 243–244

Results *See* Test results

RFC 2544 test
optimizing test time 290
running classic 291
running J-QuickCheck 298

RTP encapsulation, IP Video 227

Running
cable diagnostics 32
classic RFC 2544 tests 291
FC test, automated 282
multiple tests 5

S

Safety information xxiv

SCCP 238

Service disruption time
measuring Ethernet 118
measuring Fibre Channel 258

Service layer testing, OAM 119

Setting result group and category 4

Settings, Quick Config 28

Signal results, Ethernet 354, 399

Signaling tables, video 226

SIP
defined 238
test settings 238

SONET test results
T1.231 380

Specifying test parameters 2

SPTS, about 203

SSM *See* Sync Status Messages

Stacked VLAN
configuring 55
filtering traffic 59
results 361, 364

Starting and stopping tests 3

Streams Pipe
Multiple Streams 169
Triple Play streams 182
Summary results 340
Support xxiv
Sync Status Messages 386
SyncE
See Synchronous Ethernet
Sync Status Messages 386
Synchronous Ethernet testing 132–133
System Recovery testing, about 288

T

T1.231 results 380
T-Carrier testing
features and capabilities 140
TCP/UDP test results 395
L4 Filter Counts 395
L4 Filter Stats 395
L4 Link Stats 393
TCP/UDP testing
about 148
applications 149
ATP listen port 150
automated 282
capturing packets 93, 244
classic RFC2544 test 291
configuring layer 4 traffic 152
configuring the traffic load 154
features and capabilities 148
filter settings 155
filtering traffic 155
inserting errors 157
looping back traffic 157
Running automated Throughput test 321
running TCP Host Script 187
specifying frame length 154
specifying layer 2 and 3 settings 152
specifying packet length 154
traffic loads 64
transmitting traffic 157
well known ports 153
Wirespeed 158
Technical assistance xxiv
Test applications
Ethernet 26
Fibre Channel 250
IP 26
IP Video 215
Loop back 194
Loopback 194
MiM 27, 28
Multiple Streams 168
selecting 2
specifying parameters 2
TCP/UDP 149
Triple Play 181
Test results
1G Pair Status 353
about 10 Gigabit WAN 345
about Ethernet 345
about Fibre Channel 345
about graphs 5
about IP 345
about IP Video 207, 397
about MiM 125, 345
about MPLS 346
about NewGen 346
about VoIP 232
about VPLS 345
about Wander 396
Cable Diagnostic 351
changing layout 4
collapsing 4
custom 5
event logs 5
expanding 4
Fault 352
histograms 4
J-Profiler 395
MDI/MDIX Pair Status 351
Pair Skew 353
populating custom 5
setting category 4
setting group 4
setting the group and category 4
Summary 340
Time 415
using entire screen 4
viewing 4
viewing cable diagnostic 33
Wander 396
Test settings
H.323 239, 240
SCCP 238
SIP 238
VoIP 238–241
Testing
configuring parameters 2
connecting instrument to circuit 3
jitter and wander 140
selecting an application 2
starting a test 3
turning laser ON or OFF 3
viewing results 4
Threshold settings, IP Video 219
Time results 415
Traceroute, running 91
Traffic loads
about Ethernet 64
about Fibre Channel 256
about MiM traffic 130
transmitting bursty 65
transmitting constant 64
transmitting ramped 67
Transmitting
wander 140
Transparency testing
about loop backs 75
configuring near end 75
initiating the loop back 77
observing results 78
results 366
starting the frame sequence 78
using Quick Config 76
verifying layer 2 74
Triggers 97
Triple Play testing
about test results 183
applications 181
characterizing services 184
features and capabilities 166
graphical results, changing properties 183
graphical results, viewing 183
LEDs 182
looping back streams 187
specifying layer 2 and layer 3 settings 186

Streams Pipe 182
transmitting streams 186

Troubleshooting
general 419
tests 418

TrueSAM 264–278

Turning ON or OFF, laser 3

U

UDP
encapsulation, IP Video 227
traffic, transmitting 157

V

Video
content issues, symptoms 225
transport network problems, symptoms 226

Viewing
cable measurements 33
histograms 5
test results 4

VLAN testing
automated 317
encapsulation settings 50, 54, 79, 237
incrementing IDs for multiple streams 178

VoIP
about 230
button colors, explained 234
button colors, illustrated 234
calls, placing 243
calls, receiving 243–244
filters 241
navigating the display 235
settings, specifying 238–241
understanding test results 232

VPLS testing
about results 345
encapsulation settings 50, 55
loop back settings 192
overview 29
specifying labels 49, 237

W

Wander testing
about 140
analysis 142
exporting data 145
features and capabilities 140

Well known ports 153

Wirespeed testing 158

JDSU

Network and Service Enablement Regional Sales

North America	Latin America	Asia Pacific	EMEA	www.jdsu.com
Toll Free: 1 855 ASK JDSU	Tel: +55 11 5503 3800	Tel: +852 2892 0990	Tel: +49 7121 86 2222	

22046564
Rev. 005, February 2015
English